

LOSS ALLOCATION RULES IN THE ELECTRONIC PAYMENT SYSTEMS:  
CONSUMER PROTECTION APPROACHES IN MALAYSIA, THE UNITED  
KINGDOM AND THE UNITED STATES OF AMERICA

ADILAH ABD RAZAK

PhD

THE UNIVERSITY OF EDINBURGH  
SCHOOL OF LAW

2007



## Declaration

This thesis is submitted in partial fulfilment of the requirements for the Degree of Doctor of Philosophy in Law at the University of Edinburgh.

I hereby declare that this thesis embodies the results of my own work and follows normal academic conventions, I have made due acknowledgement of the works of others.

I also hereby declare that this piece of work has not been submitted for any other degree or professional qualification.

Signed .

Date ..... 25th June 2007 .....



## **Abstract**

Electronic payment systems are an important part of the electronic commerce infrastructure. However, like the conventional systems, they are also prone to the risk of fraudulent payments that impose financial losses on the participants. Therefore, it is important that the losses are fairly and properly allocated between the parties, to enable them to receive benefit from the systems.

In so far as the consumer and the electronic payment issuer are concerned, the losses are commonly allocated through the terms of their contract. Since contractual loss allocation may prejudice the consumer, loss allocation rules were introduced to supplement the process of allocating the losses between them. These specifically drafted loss allocation rules are influenced by the loss allocation principles, and employ a combination of liability rules including the capped liability rule, and/or fraud-based rule and/or negligence-based rules. Apart from that, the loss allocation regimes also employ the rules governing the use of an exclusion clause or unfair contract terms to protect the consumer against unfair contractual loss allocation.

It should be noted that although the loss allocation models are identical, yet their detailed rules vary from one jurisdiction to the next. Despite the differences, they share a common aim, i.e., to prescribe the rights and

liabilities of the parties in relation to the losses. In particular, they provide protection to the consumer against unfair loss allocation.

The success of the different loss allocation regimes in achieving the said objectives, in view of the different stature of the consumer and the issuer in terms of their knowledge and financial ability, depends, among others things on the clarity and the practicality of the rules and also the ability of the rules to induce the parties' precautionary action. More importantly, a perfect loss allocation scheme must be comprehensive, in the sense that there should not be any room left for the issuer to manoeuvre around its rules to unfairly use its contract terms to allocate the losses to the consumer. Failure of the rules to have these characteristics affects the protection of the consumer against fraudulent payment losses, hence the need for review and reform.

## **Acknowledgements**

I would like to express my sincere thanks and gratitude to my family, friends and supervisors who by their support, guidance and motivation keep me going till completion. Above all, I dedicated this work to my late father Abd Razak bin Yunus and my mother Minah binti Kadir.

I also would like to express my utmost gratitude to my supervisors Dr Parker Hood and Dr Charlotte Waelde for their invaluable guidance and advice. Last but not least, to Mr Andres Guadamuz for his views and comments.

On a personal note, I thank my family and loved ones, especially my husband, Ismail Abd Rahman, whose presence and absence have been a constant support and source of motivation, strength and care.

Adilah Abd Razak

July 2006.

# TABLES OF CONTENTS

	<b>DECLARATION</b>	i
	<b>ABSTRACT</b>	ii-iii
	<b>ACKNOWLEDGEMENTS</b>	iv
	<b>TABLE OF CONTENTS</b>	v-xiv
	<b>LIST OF ABBREVIATIONS</b>	xv-xvii
 <b>CHAPTER INTRODUCTION</b>		
<b>1</b>	<b>INTRODUCTION</b>	1-4
<b>2</b>	<b>REGULATING LOSS ALLOCATION: BACKGROUND POLICIES AND MODELS OF LOSS ALLOCATION RULES</b>	4-7
	<b>A Background Policies</b>	4-7
	<i>(a) Information Asymmetry and market failure</i>	5
	<i>(b) The effect of standard form contract</i>	6
	<i>(c) Fair Dealing</i>	6-7
	<b>B Models of Loss Allocation Regulations in the United States, the United Kingdom and Malaysia</b>	7-11
	<i>(a) Models based on loss allocation principles</i>	9
	<i>(b) Liability assessment depends on many liability rules</i>	10

	<i>(c) The terms of the contract for the electronic payment facilities are subjected to the regulations of the contract terms</i>	11
--	---	----

3	<b>RESEARCH OBJECTIVES AND RESEARCH METHOD</b>	11-13
4	<b>CHAPTERS' ARRANGEMENT</b>	13-14

## **CHAPTER ONE THE ELECTRONIC PAYMENT SYSTEMS AND THE RELATIONSHIP BETWEEN THE CONSUMER AND THE ISSUER**

1	<b>INTRODUCTION</b>	15-18
2	<b>ELECTRONIC PAYMENT SYSTEMS</b>	18-22
3	<b>ELECTRONIC PAYMENT SYSTEMS AND THE PARTIES' RELATIONSHIP</b>	22-32
	<b>A Electronic Funds Transfer</b>	22-24
	<b>B Credit Card Payment</b>	25-27
	<b>C Internet-based and Mobile-based EFT and Credit Card Payment</b>	27-32
4	<b>THE LEGAL RELATIONSHIP OF THE CONSUMER AND THE ISSUER</b>	32-37

**CHAPTER TWO    LOSS ALLOCATION RULES AND THE  
MEANS OF ACCESS**

<b>1</b>	<b>INTRODUCTION</b>	<b>39</b>
<b>2</b>	<b>THE PAYMENT MANDATE AND THE MEANS OF ACCESS</b>	<b>39-43</b>
<b>3</b>	<b>THE PAYMENT MANDATE AND THE LOSS ALLOCATION RULES IN THE UNITED STATES</b>	<b>43-54</b>
	<b>A    The Scope of Unauthorised Payment Mandate in the TILA</b>	<b>43-50</b>
	<b>B    The Scope of the Payment Mandate in the EFTA</b>	<b>50-54</b>
<b>4</b>	<b>THE PAYMENT MANDATE AND THE LOSS ALLOCATION RULES IN THE CCA, THE BANKING CODE AND THE DSRs IN THE UNITED KINGDOM</b>	<b>54-59</b>
	<b>A    The Scope of the Payment Mandate in the CCA and the DSRs</b>	<b>54-57</b>
	<b>B    The Scope of the Payment Mandate in the Banking Code</b>	<b>57-59</b>
<b>5</b>	<b>THE PAYMENT MANDATE AND THE LOSS ALLOCATION RULES IN THE MALAYSIAN CC GUIDELINES AND EFT GUIDELINES</b>	<b>60-64</b>

	<b>A The Scope of the Payment Mandate in the CC Guidelines</b>	60-61
	<b>B The Scope of the Payment Mandate in the EFT Guidelines</b>	61-64
<b>6</b>	<b>COMPARISON AND CONCLUSION</b>	64-68
<b>CHAPTER THREE THE MANDATE RULES IN THE CREDIT CARD AND THE EFT PAYMENT</b>		
<b>1</b>	<b>INTRODUCTION</b>	69
<b>2</b>	<b>THE MANDATE RULES IN THE UNITED STATES</b>	70-95
	<b>A Unauthorised Credit Card and EFT Payment and the Actual Authority</b>	70-76
	<i>(a) Transfer of the consumer's card and/or the PIN to the user</i>	72-75
	<i>(b) Additional cardholder and actual authority</i>	75-76
	<b>B Unauthorised Credit Card and EFT Payment and the Apparent Authority</b>	76-95
	<i>(a) Apparent authority, notice to terminate the authority and the return of an access device</i>	78-85
	<i>(b) Apparent authority and the person to be served with the notice of termination of authority</i>	85-89
	<i>(c) Apparent authority and the duty to examine the statement of account</i>	89-95

<b>3</b>	<b>THE MANDATE RULES IN THE UNITED KINGDOM</b>	<b>95-118</b>
<b>A</b>	<b>Unauthorised Credit Card and EFT Payment and Actual Authority</b>	<b>98-104</b>
	<i>(a) Transfer of the consumer's card and/or the PIN to the user</i>	<i>98-100</i>
	<i>(b) Additional cardholder and actual authority</i>	<i>100-104</i>
<b>B</b>	<b>Unauthorised Credit Card and EFT Payment and Apparent Authority</b>	<b>105-118</b>
	<i>(a) Apparent authority, notice of termination and the return of the access card</i>	<i>106-110</i>
	<i>(b) Apparent authority, negligence and the management of the access device</i>	<i>110-115</i>
	<i>(c) Apparent authority, negligence and the duty to examine the statement of account</i>	<i>115-118</i>
<b>4</b>	<b>THE MANDATE RULES IN MALAYSIA</b>	<b>118-142</b>
<b>A</b>	<b>Unauthorised Credit Card and EFT Payment and Actual Authority</b>	<b>120-123</b>
	<i>(a) Transfer of the consumer's access device and/or code to the user</i>	<i>121-123</i>
	<i>(b) Additional cardholder and actual authority</i>	<i>123-125</i>
<b>B</b>	<b>Unauthorised Credit Card and EFT Payment and Apparent</b>	<b>125-142</b>



## **Authority**

<i>(a) Apparent authority, notice of termination of authority and the return of the card to the issuer</i>	126-132
<i>(b) Apparent authority and the duty to examine the statement of account</i>	132-135
<i>(c) Apparent authority, duty of care and access code confidentiality</i>	135-138
<i>(d) Apparent authority and strict duty to maintain access code confidentiality</i>	138-142

<b>5</b>	<b>COMPARISON AND CONCLUSION</b>	142-153
<b>A</b>	<b>Transfer of Mode of Access and the Authority to Initiate Payment</b>	144
<b>B</b>	<b>Notification Rule and Termination of Authority to Initiate the Payment</b>	145-147
<b>C</b>	<b>The Person to be Served with Notification</b>	147-148
<b>D</b>	<b>The Scope of the Notification Rule</b>	148-149
<b>E</b>	<b>Negligence and Loss Allocation</b>	149-150
<b>F</b>	<b>Strict Duty to Protect Access Code Confidentiality</b>	150-153

**CHAPTER FOUR                      LOSS ALLOCATION RULES, RECEIPT OF  
BENEFIT, FRAUD    AND THE BURDEN OF PROOF**

	<b>PART I      RECEIPT OF BENEFIT AND FRAUD</b>	<b>154-181</b>
<b>1</b>	<b>INTRODUCTION</b>	<b>154-155</b>
<b>2</b>	<b>LOSS ALLOCATION BASED ON RECEIPT OF BENEFIT</b>	<b>155-172</b>
	<b>A    Unjust Enrichment, Agency of Necessity and “No Profit from           Fraud Rule” in the United States</b>	<b>155-165</b>
	<b>B    Unjust Enrichment, Agency of Necessity, and “No Profit from           Fraud” Rule in the United Kingdom and Malaysia</b>	<b>165-173</b>
<b>3</b>	<b>LOSS ALLOCATION AND CONSUMER FRAUD</b>	<b>173-178</b>
<b>4</b>	<b>COMPARISON AND CONCLUSION</b>	<b>178-181</b>
	<b>PART II    LOSS ALLOCATION AND THE BURDEN OF PROOF</b>	<b>182-226</b>
<b>1</b>	<b>INTRODUCTION</b>	<b>182-185</b>
<b>2</b>	<b>PROVING AUTHORISED PAYMENT</b>	<b>185-196</b>
	<b>A    Proof of Authority to Initiate Payment</b>	<b>185-189</b>
	<b>B    Proving the Functionality of the Access Device, Code and the           Electronic Payment System Security as Proof of Payment           Validity</b>	<b>190-193</b>
	<b>C    Proof of Receipt of Benefit</b>	<b>193-196</b>

<b>3</b>	<b>PROOF OF CONSUMER'S NEGLIGENCE OR FRAUDULENT ACTION AS AN EXCEPTION TO THE CAPPED LIABILITY</b>	<b>197-203</b>
	<b>A Proof of Negligence</b>	<b>197-199</b>
	<b>B Proof of Fraud</b>	<b>199-202</b>
<b>4</b>	<b>PROOF OF PRE-CONDITIONS FOR ALLOCATING LOSSES TO CONSUMER</b>	<b>203-218</b>
	<b>A Proof of Acceptance of the Access Device or Code</b>	<b>203-206</b>
	<b>B Proof of the Issuance of an Identification Method</b>	<b>207-211</b>
	<b>C Warning of Potential Liability</b>	<b>211-214</b>
	<b>D Proof of the Disclosure of the Notification Method</b>	<b>215-218</b>
<b>5</b>	<b>COMPARISON AND CONCLUSION</b>	<b>218-226</b>

## **CHAPTER FIVE                      LOSS ALLOCATION AND UNFAIR CONTRACT TERMS**

<b>1</b>	<b>INTRODUCTION</b>	<b>227-231</b>
<b>2</b>	<b>COMMON RULES AND THE ENFORCEABILITY OF CONTRACT TERM</b>	<b>231-235</b>
	<b>A Incorporation</b>	<b>231-233</b>
	<b>B Construction</b>	<b>233-235</b>
<b>3</b>	<b>LEGISLATIVE INTERVENTION IN THE UNITED STATES</b>	<b>236-241</b>

	<b>A Procedural Unconscionability</b>	238-239
	<b>B Substantive Unconscionability</b>	239-241
<b>4</b>	<b>LEGISLATIVE INTERVENTION IN THE UNITED KINGDOM</b>	241-252
	<b>A Unfair Contract Terms Act 1977</b>	241-247
	<b>B Unfair Terms in Consumer Contract Regulations 1999 (the “UTCCR”)</b>	247-252
<b>5</b>	<b>THE MALAYSIAN POSITION</b>	253-254
<b>6</b>	<b>ANALYSIS OF THE ELECTRONIC PAYMENT CONTRACT TERMS</b>	255-297
	<b>A Contract Terms that Affect the Protection of the Consumer against Unauthorised Payment</b>	256-284
	<i>(a) Exclusion or limitation of a liability clause</i>	256-268
	<i>(b) Indemnity clause</i>	269-271
	<i>(c) Conditions of liability</i>	271-281
	<i>(i) Protection of PIN confidentiality</i>	272-275
	<i>(ii) Notification clause</i>	275-278
	<i>(iii) Return of card</i>	278-280
	<i>(d) Conclusive evidence clause</i>	280-284
	<b>B Comments on the Clauses from the Perspective of the Unfair Terms Rules in the United States and United Kingdom</b>	284-296

	<i>(a) Complex language and jargons</i>	284-288
	<i>(b) Exclusion and indemnity clause</i>	288-291
	<i>(c) Onerous terms and conditions and conclusive evidence clause</i>	291-296
<b>7</b>	<b>COMPARISON AND CONCLUSION</b>	297-303
	<b>CHAPTER SIX REFORM ISSUES AND SUGGESTIONS</b>	
<b>1</b>	<b>SUMMARY</b>	304
<b>2</b>	<b>REVIEW AND RECOMMENDATIONS FOR REFORM</b>	304-324
	<b>A The Policy of Loss Allocation</b>	305-306
	<b>B Weakness in the Substance</b>	307-321
	(a) The scope of unauthorised payment	307-310
	(b) Negligence and strict confidentiality as a basis of liability	310-311
	(c) Notification rules	311-314
	(d) Burden of proof	314-317
	(e) Examination of the account statement	317-318
	(f) Unfair terms regulations	318-321
	<b>C Implementation and Enforcement Weaknesses</b>	321-324
	<b>REFERENCES</b>	325-341
	<b>APPENDICES</b>	
	<b>A Credit Card Guideline</b>	
	<b>B Guidelines on Consumer Protection on Electronic Funds Transfers</b>	

## LIST OF ABBREVIATIONS

A. L. R.	American Law Reports
A.L.R. Fed	American Law Reports Federal
Ala. L. Rev	Alabama Law Review
All ER	All England Report
Am. Bankr. L.J	American Banker Law Journal
Am. Bus. L.J	American Business Law Journal
Am. Jur.	American Jurisprudence
Am. Rev. Int'l Arb.	American Review of International Arbitration
AMR	All Malaysian Review
Ann. Rev. Banking L.	Annual Review of Banking Law
CC Guidelines	Credit Card Guidelines
CCA	Consumer Credit Act 1974
CLJ	Current Law Journal
Colum. Bus. L. Rev	Columbus Business Law Review
DSRs	Consumer Protection (Distance Selling) Regulations 2000
EFT Guidelines	Guidelines on Consumer Protection on Electronic Fund Transfers
EFTA	Electronic Funds Transfer Act 1978
EWCA Civ	Court of Appeal Civil Division
FRB	Federal Reserve Board

Geo. L.J.	Georgetown Law Journal
Harv. L. Rev	Harvard Law Review
J. I. B. L	Journal of International Business Law
J.B.L.	Journal of Business Law
L.Q.R.	Law Quarterly Review
Law & Hist. Rev	Law and History Review
Mich. L. Rev	Michigan Law Review
MLJ	Malayan Law Journal
MLJU	Malayan Law Journal Unreported
MLR	Modern Law Review
N.Y.U. J. Legis. & Pub. Pol'y	New York University Journal of Legislation & Public Policy
Stat. Law	Statute Law Review
Tex. L. Rev	Texas Law Review
TILA	Truth in Lending Act 1968
Tul. L. Rev	Tulane Law Review
U. Chi. L. Rev	University of Chicago Law Review
U. Colo. L. Rev	University of Colorado Law Review
U. Pa. L. Rev.	University of Pennsylvania Law Review
U. Pitt. L. Rev	University of Pittsburgh Law Review
UCC	Uniform Commercial Code
UCTA	Unfair Contract Terms Act 1977
Utah L. Rev	Utah Law Review

UTCCR

Unfair Terms in Consumer Contract Regulations

1999

Wm. & Mary L. Rev

William and Mary Law Review

Yale L. J.

Yale Law Journal



# INTRODUCTION      LOSS    ALLOCATION    AND    CONSUMER PROTECTION ISSUES IN THE ELECTRONIC PAYMENT SYSTEMS

## 1      INTRODUCTION

Electronic commerce activities in the 21<sup>st</sup> century have moved beyond the Electronic Data Interchange model to an open electronic commerce model where the public at large participate through the use of Internet and mobile commerce (the m-commerce) systems.<sup>1</sup> However, sophisticated as it sounds, the electronic commerce market, just like the traditional commerce model, also requires support from other economic market infrastructures for its success.<sup>2</sup> One of these important infrastructures is the payment system, which historically, is proven to be essential in every economic market.<sup>3</sup>

Generally, payment systems, conventional and electronic, contribute to commercial activities by facilitating the process of making the payment. Through the payment

---

<sup>1</sup> Wigand, R. T., "Electronic Commerce: Definition, Theory, and Context", (1997) *the Information Society*, Volume 13, NO. 1, 1-7, and Tarasewich, P. *et al.*, "Issues in Mobile E-Commerce", (2002) *Communications of the Association for Information Systems*, Volume 8, at 41-64.

<sup>2</sup> Mesenbourg, T. L., "Measuring Electronic Business: Definitions, Underlying Concepts, and Measurement Plans" US Census Bureau, at <<http://www.census.gov/epcd/www/ebusines.htm>> (Visited 26<sup>th</sup> April 2006) and also Singh, A. D., "Electronic Commerce: Some Implications for Firms and Workers in Developing Countries", (2000), 10, *The International Institute for Labour Studies Discussion Paper*, at <<http://www.ilo.org/public/english/bureau/inst/download/dp12300.pdf>> (Visited 1<sup>st</sup> April 2006).

<sup>3</sup> See Davies, G., *A History of Money from Ancient Times to the Present Day*, 3<sup>rd</sup> Edn with revision (2002) University of Wales Press. (Hereafter Davies, G. A., *A History of Money*) and Jevons, W. S., *Money and The Mechanism of Exchange*, 9<sup>th</sup> Edn (1890) Kegan Paul Trench, Trübner. (Hereafter Jevons, W. S., *Money and the Mechanism of Exchange*)

systems the buyer transfers money value to the seller to discharge his money obligation.<sup>4</sup>

It should be noted that because a process of making the payment involves a transfer of monetary value, the payment systems' participants are exposed to the risk of financial losses when a fraudulent payment occurs.<sup>5</sup> The risk of a fraudulent payment in the electronic payment systems can originate from many sources including illegal access to the consumer's personal details (such as the personal identification numbers (the "PIN") and the payment card details) that allows an unauthorised individual to initiate fraudulent payment.<sup>6</sup> Furthermore, a fraudster may take control of the consumer's payment mechanisms (such as the debit card and the credit card) and use the details and/or the card to initiate fraudulent payment.<sup>7</sup>

In the case of payment systems in electronic commerce, wired and mobile, the highly sophisticated communication technology used may also expose the consumer to the risk of fraud. This risk is usually created by a systems' security breach as a result of hacking,<sup>8</sup> spoofing<sup>9</sup>, sniffing<sup>10</sup> and virus or worm.<sup>11</sup>

---

<sup>4</sup> Goode, R. M., *Commercial Law* 3<sup>rd</sup> Edn (2004), 460-461, Lexis Nexis UK and Penguin. (Hereafter Goode, R. M., *Commercial Law*).

<sup>5</sup> Fraud falls within the scope of Operational Risk. See Basel Committee on Banking Supervision Consultative Document on "Operational Risk" January 2001, at <<http://www.bis.org/publ/bcbzca07.pdf>> at 2-3. (Visited 26 April 2006).

<sup>6</sup> Fry, M. J. *et al.*, *Payment Systems in Global Perspective* (1999), 4, Routledge in cooperation with the Bank of England's Centre for Central Banking Studies.

<sup>7</sup> Ibid.

<sup>8</sup> In June 2005, Mastercard had identified a system security breach at one of the payment processing company as a result of hacking activities which exposed around forty million card details to fraud. Yahoo Financial News, "MasterCard International Identifies Security Breach at CardSystems Solutions, A Third Party Processor of Payment Card Data" June 17th 2005, at <<http://biz.yahoo.com/bw/050617/175525.html?v=1>>. See *United States v. Petersen* 98 F.3d 502, 504 (9th Cir. 1996) a case involving a hacker breaking into the system of a credit-reporting agency.

<sup>9</sup> Felten, E. W., *et al.*, "Web Spoofing: An Internet Con Game" 20th National Information Systems Security Conference (Baltimore, Maryland), October, 1997, at <<<http://www.cs.princeton.edu/sip/pub>

The said computer system security risks may result in a fraudulent payment because they facilitate:

(a) an alteration to the payment message like the amount of payment and the payee's identity, (ii) a breach of confidentiality which results in unlawful access to the consumer's personal and financial information, allowing the issuance of a fraudulent payment instruction; and (iii) an impersonation, where the impostor acts as if he were an authorised user of the payment facilities or the payee.<sup>12</sup>

Various authentication technologies have been and are still being developed (purely technical systems like the digital signature, personal identification numbers (the PIN), passwords, and the electronic token and technical/personality based, such as biometric scanning technology,<sup>13</sup> and biometric recording,<sup>14</sup>) to prevent or reduce the above risks. Nonetheless, they cannot guarantee that the electronic payment systems are entirely free from the risks of fraudulent payment. Accordingly, it is necessary to

---

/index.php3> (visited 27<sup>th</sup> March, 2003). The web page of the renowned auction merchant, eBay for instance, was attacked in this way in 2002 where members were required to log in via a forged link sent in the e-mail. Internet Watchdog Warns of Fake eBay Web Site, The Mercury News, December 11<sup>th</sup> 2002 at <<http://www.siliconvalley.com/mld/siliconvalley/news/4713932.htm>> (Visited 27<sup>th</sup> March 2003).

<sup>10</sup> In October 1998, the e-mail passwords of some 4,500 students and staff at Stanford University were stolen when crackers broke into the school's security system using a data-stealing software program called a "sniffer". This software intercepts passwords as users are logging on. Kubin, L., "Stanford E-mail Cracked", November 21 1993 in Suite 101.com at <<http://www.suite101.com/article.cfm/hackers/12837>> (Visited 27<sup>th</sup> March, 2003).

<sup>11</sup> Qing, S. and Wen, W., "A survey and Trends on Internet Worms", (2005) *Computers & Security* 24, 334 -346, at 335-336, and Gobuty, D. E., "Defending Medical Information systems against Malicious Software" (2004) *International Congress Series* 1268, 96-107, at 98-99.

<sup>12</sup> Hendry, M., *Smart Card Security and Applications*, 2<sup>nd</sup> Edn (2001) 20-21, Artech House and Jung, B., *et al*, "Security Threat to the Internet: A Korean Multi-Industry Investigation" (2001) *Information & Management*, 38, 487-498, at 489.

<sup>13</sup> Ford, M. D., "Identity Authentication and 'E-Commerce'", 1998 (3) *The Journal of Information, Law and Technology (JILT)* at <http://elj.warwick.ac.uk/jilt/98-3/ford.html>> (Visited 16<sup>th</sup> December, 2003).

<sup>14</sup> Woodward, J. D., "Biometric Scanning, Law & Policy: Identifying the Concerns-Drafting the Biometrics Blueprint" (1997) 59 *U. Pitt. L Rev.* 97, for a detail discussion on biometric identification and the law.

have proper loss allocation schemes to regulate the impact of the losses caused by the fraudulent payment on both the consumer and the issuer.

## **2           REGULATING LOSS ALLOCATION: BACKGROUND POLICIES AND MODELS OF LOSS ALLOCATION RULES**

### **A           Background Policies**

Fraudulent payment imposes financial losses on all the electronic payment systems' participants, including the consumer. These losses have to be dealt with, in one way or another, to allow the consumer and the issuer to enjoy the benefits that they expect to receive from electronic payment facilities.

Generally, in the absence of a specific loss allocation scheme, fraudulent payment losses are allocated between the consumer and the issuer by their contract terms. This loss allocation approach, according to the supporters of the freedom of contract theory, is sufficient to protect the consumer against unfair allocation of losses. According to this view, bad issuers, who allocate the losses unfairly, will be pushed out of the market by consumers, lack of demand.<sup>15</sup> Even so, there are certain circumstances when consumer protection cannot entirely rely on market forces but requires legal intervention.

---

<sup>15</sup> The freedom of contract theory is best explained by the statement of George Jesse MR in *Printing and Numerical Registering Co v Sampson* (1875) LR 19 Eq 462, at 465. "If there is one thing which more than another public policy requires it is that men of full age and competent understanding shall have the utmost liberty of contracting, and their contracts entered into freely and voluntarily shall be held sacred and shall be enforced by Courts of Justice." See Scott, C. and Black, J., *Cranston's Consumers and the Law*, 3<sup>rd</sup> Edn. (2000), 22-29, Butterworths. (Hereafter Scott, C and Black, J., *Cranston's Consumers and the Law*)

(a) *Information Asymmetry and market failure.*<sup>16</sup>

In electronic payment systems, the use of sophisticated advanced computer technology creates an imbalance and unequal standing between the consumer and the issuer in terms of their knowledge of the technological characteristics of the electronic payment systems; of the functioning of the particular payment system; of the likelihood of risk within the system, and also of the impact of that risk.<sup>17</sup> As a result, the consumer would not, in most cases, be able to appreciate the effect of the contractual terms that assign to him the risk in electronic payment systems, including the risk of fraudulent payment. Moreover, the consumer's failure to understand the system and its risk means that he cannot effectively negotiate the contractual terms with the issuer who, on the other hand, can employ skilful and knowledgeable staff in its operation.<sup>18</sup>

Likewise, information asymmetry may also raise the consumer's transaction cost as it burdens the consumer with the cost of finding relevant information to be able to negotiate the contract effectively.<sup>19</sup> Therefore, in this environment, where the consumer lacks the necessary information to make informed decisions, the concept of *caveat emptor*, seems to be indefensible.

---

<sup>16</sup> Cartwright, P., *Banks, Consumers and Regulation*, (2004) 16-18, Hart Publishing. (Hereafter Cartwright, P., *Banks Consumers and Regulation*).

<sup>17</sup> Craswell, R., "Freedom of Contract", the Coase Lecture Series, at <<http://www.law.uchicago.edu/Publications/Working/WkngPprs%2026-50/33.Craswell.FrdmCtrct.pdf>> (Visited 15 March 2006).

<sup>18</sup> Harvey, B. W. and Parry, D. L., *The Law of Consumer Protection and Fair Trading*, 5<sup>th</sup> Edn. (1996), 67, Butterworths. (Hereafter Harvey B. W., and Perry, D.L., *The Law of Consumer Protection and Fair Trading*). See also Clarke, S. H., "Unmanageable Risks: Macpherson v. Buick and the Emergence of a Mass Consumer Market", (2005) 23 *Law & Hist. Rev.* 1 for a view on the risk of technological innovation on consumer. In this article the discussion was concentrated on the car.

<sup>19</sup> Government of Australia Taskforce on Industry Self-Regulation, "Industry Self-Regulation in Consumer Markets" (2000), at 18 footnote 9, at <[http://www.consumersonline.gov.au/content/selfregulation/finalreport\\_taskforce/03\\_chap2.asp](http://www.consumersonline.gov.au/content/selfregulation/finalreport_taskforce/03_chap2.asp)> (Visited 20<sup>th</sup> December 2004).

(b) *The effect of standard form contract.*

It is undeniable that to a certain extent contracting via a standard form contract, lowers the transaction cost.<sup>20</sup> However, this type of contract raises a concern as it may facilitate the use of unfair terms; terms which are one-sided and disadvantageous to the consumer's interest.<sup>21</sup> Because the relationship between the consumer and the issuer is usually done on an unequal footing, using a standard terms contract means that the consumer is forced to accept the required service upon the issuer's non-negotiable terms, which in some cases is disadvantageous to him.

(c) *Fair Dealing*<sup>22</sup>

The demand for the issuer to maintain the security of the payment systems may increase its transaction costs. Therefore, to maximise its profits, the issuer may have to transfer the cost to other parties in the transaction, including the consumer. In fact, the issuer may choose to transfer the cost indirectly by, for instance, increasing the service fees,<sup>23</sup> or it can do so by directly allocating some or all of the fraudulent payment losses to the consumer. Although the increased transaction cost may be cited to justify non-intervention, it does not mean that the rules cannot be

---

<sup>20</sup> Posner, R.A., *Economic Analysis of Law*, 6<sup>th</sup> Edn. (2003), 115, Aspen Publishers.

<sup>21</sup> Burke J. J. A., "Contract as Commodity: A Non-fiction Statutory Approach" (2000), *Stat. Law* 21 (12), 12-42 and Kronman, A. T., "Contract Law and Distributive Justice" (1980) *the Yale Law Journal*, Vol. 89, No. 3, at 472-511.

<sup>22</sup> Cartwright, P., *Banks, Consumers and Regulation*, at 16-18.

<sup>23</sup> Harvey, B. W., and Parry, D. L., *The Law of Consumer Protection and Fair Trading*, at 67.

drafted to take into account the economic factors including the cost of the parties to bear the losses<sup>24</sup> without surrendering the interest of the consumer.

Looking at the above three factors, fairness and efficiency requires the state to regulate the allocation of the losses instead of leaving them to be distributed through the issuer's contract terms.

## **B Models of Loss Allocation Regulations in the United States, the United Kingdom and Malaysia**

Apparently, state intervention in regulating electronic payment systems and the loss allocation rules varies from one jurisdiction to the other. Some jurisdictions used state-regulation, while others combined state-regulation and self-regulation.<sup>25</sup> In the United States, loss allocation in the credit card and EFT payment systems employed state-regulation models. Hence, credit card payments are regulated by the Truth in Lending Act 1968 (the "TILA"), and its implementing regulations, Regulation Z (the "Reg. Z") while the EFT payments are regulated by the Electronic Funds Transfer Act 1978 (the "EFTA") and Regulation E (the "Reg. E").<sup>26</sup>

---

<sup>24</sup> Gillette, C. P., "Rules, Standard, and Precautions in Payment Systems" (1996) *Virginia Law Review* Vol 82., 181, at 221-230.

<sup>25</sup> Black, J., "Constitutionalising Self-Regulation" (1996) 59 (1) *MLR*, at 24-55, at 27; Scott, C., and Black, J., *Cranston's Consumers and the Law* at 26 and 39.

<sup>26</sup> Regulation Z was passed by the Federal Reserve Board by virtue of s. 105(a) of the TILA to implement the TILA; Official Staff Commentary to Regulation Z Codified to 12 C.F.R. Part 226 section 226.12 (b)(1). Reg E. was passed to implement the EFTA by virtue of s. 904(a) of the EFTA; see also Regulation. 205. 1 (a) of Reg. E.



Other than those rules, the relevant rules can also be found in the law of agency based on the Restatement (Second) of Agency 1958 (the “Agency Restatement”), the law of restitution based on the Restatement (First) of Restitution 1937 (the “Restitution Restatement”) and also the common law of contract.

Compared to the United States, loss allocation in the credit card system and the EFT system in the United Kingdom combine state-regulation and self-regulation.<sup>27</sup> Hence, there is the Consumer Credit Act 1974 (the “CCA”) which is applicable to a credit token agreement<sup>28</sup> the Consumer Protection (Distance Selling) Regulations 2000 (the DSRs”) which applies to payment card,<sup>29</sup> and the Banking Code, which applies to the payment card except the store card.<sup>30</sup> Apart from that, the loss allocation regime is also supplemented by the general law of banking contracts, rules of agency, and also the regulations of unfair contract terms i.e., the Unfair Contract Terms Act 1977 (the “UCTA”) and the Unfair Terms in Consumer Contracts Regulations 1999 (the “UTCCR”).<sup>31</sup>

The Malaysian approach to loss allocation in electronic payment systems is a combination of statutory regulations and the guidelines issued by the Central Bank by virtue of its power under s. 76 (4) of the Payment Systems Act 2003. The Act

---

<sup>27</sup> When the United Kingdom is referred to it means England unless otherwise stated.

<sup>28</sup> Section 189 of the CCA 1974 provides; “credit-token agreement” means a regulated agreement for the provision of credit in connection with the use of a credit-token”. Credit token refers to “a card, check, voucher, coupon, stamp, form, booklet or other document or thing given to an individual by a person carrying on a consumer credit business” on the production of which the issuer will provide credit. See s. 14 (1) of the CCA 1994.

<sup>29</sup> Regulation 21. SI 2000/2334.

<sup>30</sup> Glossary definition of card includes “debit, credit, cheque guarantee, charge cards and cash cards. It does not include electronic purses or store cards.” Banking Code March 2005.

<sup>31</sup> SI 1999/2083. European Council Directive 93/13/EEC on Unfair Terms in Consumer Contracts *OJ L 95/ 29*.



authorises the Central Bank to enforce the Credit Card Guidelines (the “CC Guidelines”), which are applicable to credit card payment, and the Guidelines on Consumer Protection on Electronic Funds Transfer (the “EFT Guidelines”) which are applicable to the EFT payment. Apart from these guidelines, the systems are also subject to the law of agency and restitution as codified in the Contract Act 1950 (Revised 1973), and the common law rules of banking.

Despite the above minor differences, the loss allocation models in these three jurisdictions share common characteristics. These characteristics are:

*(a) Models based on loss allocation principles*

The loss allocation rules incorporated in the electronic payment regulations were modelled to fulfil three loss allocation principles, namely, loss spreading, loss reduction and loss imposition.<sup>32</sup> These three principles influence the features of the loss allocation scheme by defining the policy which determines the loss allocation rules that should be used in the allocation of the unauthorised payment losses between the consumer and the issuer. They can also be used to define the conditions and the circumstances for the sharing of the losses and also the reallocation of the losses from one party to the other.

---

<sup>32</sup> Cooter, R. D. and Rubin, E. L., “A Theory of Loss Allocation for Consumer Payments” (1987) 66 *Tex. L. Rev.* 63. (Hereafter Cooter, R.D., and Rubin, E.L., “A Theory of Loss Allocation for Consumer Payments”).

*(b) Liability assessment depends on many liability rules*

There are several bases of liability in all the electronic payment regulations discussed in this dissertation. However, the most common and prominent feature of all the loss allocation rules discussed are the agency rules, which are known as the mandate rules for the purpose of this dissertation.<sup>33</sup>

Apart from the mandate rules, there are also other liability rules which shaped the model of the loss allocation scheme in these three jurisdictions. For example, in the United States, the loss allocation rules in the EFTA and the TILA also apply the receipt of benefit rule which is based on restitution.<sup>34</sup> Other than that, the EFTA also incorporates a tort of deceit rule which allows the issuer to allocate the losses from an unauthorised payment to the consumer by proving that the payment was fraudulently made by the consumer or by a person with whom he acted in concert.<sup>35</sup> Similarly, the loss allocation schemes in the United Kingdom and Malaysia also apply various other liability rules. The UK Banking Code, for example, allocates the losses based on negligence and fraud.<sup>36</sup> The negligence rule is also incorporated in the Malaysian EFT Guidelines while the CC Guidelines allocate losses based on fraud.

---

<sup>33</sup> Section 103(o) of the TILA, s. 903(11) of the EFTA, s. 83 and s.84 of the CCA, s. 12 of the Banking Code, Para 13 of the CC Guidelines and Para 15 of the EFT Guidelines.

<sup>34</sup> Section 133 and s. 103(o) of the TILA and s. 909 and 903(11) of the EFTA.

<sup>35</sup> Section 903 (11)(B).

<sup>36</sup> Section 12.11 and 12.12 of the Banking Code, Para 13 of the CC Guidelines and Para 15 of the EFT Guidelines.

- (c) *The terms of the contract for the electronic payment facilities are subject to the regulations of the contract terms*

Because the relationship between the consumer and the issuer is contractual in nature, the contract terms may be used to unfairly allocate the fraudulent payment losses to the consumer. Therefore, the consumer can only be saved from the issuer's unfair loss allocation practices if the respective regulations expressly and clearly invalidate any term that violates the regulatory loss allocation rules. Where the regulations fail to invalidate such practices, there is the potential for the issuer to use its contract terms to directly or indirectly allocate the losses to the consumer even if such practices contradict the respective regulations. In this regard, it is believed that the law that regulates the enforceability of unfair contract terms becomes one important aspect of the loss allocation regime in the electronic payment systems.

### **3 RESEARCH OBJECTIVES AND RESEARCH METHOD**

Earlier on, it was mentioned that the risk of financial losses might affect the utility of the electronic payment systems to the participants including the consumer. Moreover, it was also shown that regulating the process and the method of loss allocation is important for the protection of the consumer against unfair allocation of unauthorised payment losses.

Based on the above observations, this research focuses on the loss allocation rules in

the electronic payments regulations in Malaysia in comparison to such rules as apply in the United States of America and the United Kingdom. The aims are to

1- understand the different loss allocation rules used in the different type of electronic payment systems;

2 – examine the applicability of the rules in the electronic payment systems for electronic commerce;

3 – identify the strength and weakness of the different rules in different jurisdictions in order to assess their impact on the consumer, in the conventional market and also - in the electronic commerce market;

4- identify and address with clarity, the inadequacy of consumer protection regulations in Malaysia, and

5 – suggest changes to the existing Malaysian regulations in order to improve the protection of the consumer against fraudulent payment in electronic payment systems and to bring them in line with the standard applicable at the international level.

In order to achieve these objectives, this research adopts a comparative analysis of existing electronic payment systems' regulations in Malaysia, in comparison to the regulations in the United States and the United Kingdom. A comparative approach was thought to be necessary as it would allow a detailed examination of the various

approaches adopted in the loss allocation rules that are used in these jurisdictions. Comparative law, according to Lepaulle,<sup>37</sup> enables an individual to see the law of his country through the eyes of a stranger, by allowing him “[t]o see things in their true light”. Furthermore, by applying a comparative method of analysis, it allows for an observation of “...how other societies at a similar stage of civilisation face up to the same and corresponding problems”.<sup>38</sup>

Hence, comparative analysis was applied to all applicable rules and regulations. Apart from that, to assist in the interpretation of the rules, reference was also made to judicial decisions in which the rules were discussed. In this way, the practical application of the loss allocation rules could be fully appreciated.

#### **4 CHAPTERS’ ARRANGEMENT**

There are six chapters in this dissertation. The dissertation begins with the introductory chapter that explains the research background including the research issues, the research method and objectives and also the chapters arrangement.

Chapter one of the dissertation describes the electronic payment systems in detail. It also illustrates through various diagrams the electronic payment systems models, and the legal relationship between the consumer and the issuer.

---

<sup>37</sup> Lepaulle, P., “The Function of Comparative Law: with a Critique of Sociological Jurisprudence” (1922) 35 *Harvard Law Review* 838, at 858.

<sup>38</sup> Walker, D. M. , *The Scottish Legal System: an Introduction to the Study of Scots Law*, 8<sup>th</sup> Edn Revised (2001), 21, W. Green/Sweet & Maxwell.

Chapter two discusses the loss allocation rules from the perspective of the method of issuing the payment mandate. A detailed discussion involving the application of the mandate or agency rules begins in Chapter three. Here the legal nature of the relationship between the consumer and the issuer is analysed from the perspective of the actual authority and the apparent authority of the person who initiated the disputed payment.

The discussion is continued in Chapter four by focusing on the loss allocation rules that found their basis in the law of restitution, and in the tort of deceit. This chapter also discusses the relationship between the burden of proof and the loss allocation rules.

Chapter 5 discusses the exclusion clause and the unfair contract terms. In this chapter the terms used by the issuer in the contract for the credit card and debit card payment facilities were analysed to identify the effect of using them on the protection of the consumer against fraudulent payment losses. This discussion also reveals the impact of the failure to implement the CC and EFT Guidelines on the consumer.

Finally, Chapter 6 concludes the research by summing up its findings. It also contains suggestions and recommendations thought to be essential in order to improve the protection of consumers against unauthorised payment in the electronic payment systems in Malaysia.

# CHAPTER ONE THE ELECTRONIC PAYMENT SYSTEMS AND THE RELATIONSHIP BETWEEN THE CONSUMER AND THE ISSUER

## 1 INTRODUCTION

The relationship between a consumer and a merchant in any economic market falls into the category of an exchange relationship, a relationship where each of them expects to receive comparable benefit from one another.<sup>1</sup> While the consumer receives goods or services, the merchant benefits from a payment. In this context, the payment serves as a medium of exchange of value between the contracting parties. Moreover, since goods and services are nowadays priced in terms of money value, a payment discharges the money obligation owed by the payor to the payee.<sup>2</sup>

From the above perspectives, it is apparent that payment is a necessary component of economic activity. Further evidence of the function of payment in economic activities can also be observed by exploring the history of payment systems.

Traditionally, when each member of society was a producer and user at the same time, individuals depended on one another for their needs. Therefore, when two of them had a “double coincidence of want”, they bartered the commodities with one another.<sup>3</sup> Later, when society started to attach value to things other than the

---

<sup>1</sup> Clark, M. S. *et al.*, “Keeping Track of Needs in Communal and Exchange Relationships”, *Journal of Personality and Social Psychology*, 51,2 (1986) 333-338.

<sup>2</sup> Goode R. M., *Commercial Law*, at 460-461.

<sup>3</sup> Jevons, W. S., *Money and the Mechanism of Exchange* 9<sup>th</sup> Edn. (1890) at 3-4, Kegan Paul Trubner.

commodities, items such as cowry shells, beads and tobacco were used as exchange mechanisms.<sup>4</sup>

Further developments in payment history involved the use of precious metal such as gold and silver as an exchange mechanism to discharge the monetary obligation.<sup>5</sup> The transformation continued to take place when paper currency was introduced to remedy the problem of transportation and security associated with the transfer of valuable metal, especially in distance travelling.<sup>6</sup>

Progress in payment history reflects the changes of the medium that constitutes what is called money. Nowadays, however, it is the method of transferring money that is being transformed. This procedure, which refers to the moment where the money or the monetary value is transferred from one party to another, is called the payment system.<sup>7</sup>

The old form of transferring the monetary value, which is still in use today, is a cash transfer of the currency. Then, the currency represented the value of gold or silver kept by the issuer.<sup>8</sup> Nowadays, it is the transfer of fiat money which is valuable, due to the concept of legal tender.<sup>9</sup>

---

<sup>4</sup> Hingston Q. A., *A Survey of Primitive Money: The beginnings of Currency* (1949) Methuen & Co. Ltd. (Hereafter Hingston, Q. A., *A Survey of Primitive Money*).

<sup>5</sup> Supra n 3, at 34.

<sup>6</sup> Supra n 3 at 197-200.

<sup>7</sup> Supra n 3 at 34. See also Bank of England, "Payment Systems Oversight Report 2004", (January 2005) Issue 1 at <<http://www.bankofengland.co.uk/publications/psor/psor2004.pdf>>, at 7 (Visited 26<sup>th</sup> April 2006).

<sup>8</sup> Supra n 3, Chapter 17.

<sup>9</sup> Proctor, C., *Mann on The Legal Aspect of Money*, 6th Edn. (2004), 42, Clarendon Press.



Another mode of payment that relies on the transfer of a material which represents money value is the use of bills of exchange.<sup>10</sup> The most popular type of bill is the cheque. In this system, the thing that is transferred is not the money but the value of the debt owed by the drawee to the drawer.<sup>11</sup>

Payment by a cash transfer of the fiat currency and by using the bills, displayed a common reliance in both payment systems on the use of paper as a communication medium. The shared characteristic of the two different payment systems shows a strong connection between the payment systems and the communication method. Therefore, it is not surprising to see the many changes introduced by the development of the electronic communication system in the payment systems.

Although, electronic communication technology was introduced to the banking industry as early as 1866,<sup>12</sup> it is only the development of the Electronic Funds Transfer system (the "EFT") that directly benefits the consumer.<sup>13</sup> Through this system, the consumer is presented with many new payment services including EFT payment with a debit card and EFT payment at the point of sale (EFTPOS).<sup>14</sup>

---

<sup>10</sup> Holden J. M., *The History of Negotiable Instruments in English Law* (1955) 1-2, University of London The Anthlon Press. See the definition of the bills of exchange in s 3(1) of the United Kingdom Bills of Exchange Act 1882,

<sup>11</sup> Kahn, C. M. and Roberds, W., "The Economic of Payment Finality", (2002) *Federal Reserve Bank of Atlanta Economic Review*, Issue 2, 1-12. See s. 73 of the UK Bills of Exchange Act 1882 which explained the concept of a payment by cheque.

<sup>12</sup> Alston, H. C., "Electronic Banking: Will That Be Cash, Credit, or E-money?" (1997) 1 *N.C. Banking Inst* 225 at 228.

<sup>13</sup> See Chorafas, D. N., *Electronic Funds Transfer* (1988), 99, Butterworth & Co (Publishers) Ltd; Pang, J., *Banking and Finance in Malaysia* (1995), 21, Federal Publication Sdn Bhd for the history of the EFT.

<sup>14</sup> Hooley, R. and Taylor, J., "Payment by Funds Transfer", in Brindle, M. and Cox, R. (Eds), *Law of Bank Payments*, 3rd Edn. (2004) Ch 3, Para 3-026, Sweet & Maxwell. (Hereafter Brindle, M. and Cox, R., *Law of Bank Payments*).

The EFT system is not the only electronic payment system developed for the consumer. In fact, many other systems have been developed and are still being developed to facilitate consumer transactions. Therefore, it is necessary to study the types of payment systems that are covered by this dissertation, which focuses on the loss allocation rules and consumer protection in electronic payment systems.<sup>7</sup>

## **2 ELECTRONIC PAYMENT SYSTEMS**

Electronic payment systems can be divided into the wholesale system and the retail system.<sup>15</sup> The latter system offers many payment facilities to the consumer namely, debit and credit transfer via the EFT, the EFTPOS payment, payment via a credit card, and a debit card and also electronic payment via the internet and mobile-devices such as the mobile phone (the “m-payment”).<sup>16</sup>

These payment facilities may be used together or independently. For example, the EFT payment can be made at an ATM machine or through the internet by using internet banking services. Similarly, a debit card payment can also be made through the EFT system, the internet or the m-payment system. The same also goes for the credit card.

---

<sup>15</sup> See the characteristics of retail payment system, in Bank for International Settlements Committee on Payment and Settlement Systems, “Retails Payment in Selected Countries: A Comparative Studies” September 1999 at <<http://www.bis.org/publ/cpss33.pdf>> at 2-5 (Visited 10<sup>th</sup> December 2004). Mann, R. J., *Payment Systems and other Financial Transactions: Cases, Materials, and Problems*, 2<sup>nd</sup> Edn. (2003) Ch. 2, at 157-227, Aspen Law & Business. (Hereafter Mann, R. J., *Payment Systems and other Financial Transactions: Cases, Materials, and Problems*).

<sup>16</sup> Herzberg, A., “Payments and Banking with Mobile Personal Devices”, *Communications of the ACM* (May 2003), Vol 46 , Issue 5, at 53 – 58.

The consumer electronic payment can be further divided into two general classes, namely, an account-based system or a notational system, and a token system.<sup>17</sup> The account-based system is a payment that requires the creation of an account with the payment service provider, bank or otherwise. In this system, when the payment is initiated, the consumer is sending information that authorises the service provider to debit the consumer's account with the value of the intended payment.<sup>18</sup> Thus, payment by cheque, credit card, debit card and debit transfer falls under the notational system.<sup>19</sup> Some new internet and m-payment systems such as the e-dinar systems,<sup>20</sup> and the Moxmo systems,<sup>21</sup> are also account-based systems.

A token system, on the other hand, operates like a cash payment because the transfer that occurs involves the transfer of the actual money value not a transfer of the payment information.<sup>22</sup> The money value resides either in a physical product such as a stored-value card or a smart card, a digital wallet or purse which contains a microprocessor chip that performs a data-processing function, or in the form of an electronic impulse that is stored in the consumer's computer.<sup>23</sup> Some examples of

---

<sup>17</sup> Camp, L. J., *Trust and Risk in Internet Commerce* (2000), 184, The MIT Press (Hereafter Camp, L. J., *Trust and Risk in Internet Commerce*); Welling, S. N. and Rickman, A. G., "Cyberlaundering: The Risks, The Responses", (1998) 50 *Fla. L. Rev.* 295, and Stevenson, R. B. Jr., "The Regulation of Electronic Payment Systems: Ten Obvious Observations" (1998) *Glasser LegalWorks* 117, at 119.

<sup>18</sup> Ibid, Camp, L. J., *Trust and Risk in Internet Commerce*.

<sup>19</sup> Medvinsky, G. and Neuman, C., "NetCash: a design for practical electronic currency on the Internet", (1993) Proceedings of the 1st ACM conference on Computer and Communications Security.

<sup>20</sup> E-dinar web page at <[http://www.e-dinar.com/html/3\\_2.html](http://www.e-dinar.com/html/3_2.html)> (Visited on 26th April 2006).

<sup>21</sup> Cited in Mallat, N., *et al.*, "Mobile Banking Services", (2004) *Communications of the ACM* Volume 47, Number 5, 42-46.

<sup>22</sup> Camp, L. J., *Trust and Risk in Internet Commerce*.

<sup>23</sup> Ibid.

the token system include the failed Mondex card, Internet Cash Secure Prepaid Card, and KLELine electronic cash system.<sup>24</sup>

Another way of classifying the electronic payment systems is by looking at the electronic communication model they use. Hence, there is an m-payment system and also the wired payment system, a system which depends on wired communication technology.<sup>25</sup> The difference between these two types of payment systems is that in the m-payment system, the consumer can make a payment through a mobile terminal such as a mobile phone and personal digital assistant (PDA)<sup>26</sup> while in the connected system, the payment information has to pass through a wired communication terminal such as a computer that is connected to the banking institution's intranet.

Just like the connected payment system, an m-payment system also uses an account-based model and a token-based model including an embedded smart card payment, an EFT transfer, a credit card payment, and payment via a mobile phone pre-paid voucher.<sup>27</sup>

---

<sup>24</sup> Hance, O. and Balz, S. D., *the New Virtual Money: Law and Practice* (1999) at 25-31 and 44-48, Kluwer Law International.

<sup>25</sup> Junseong, A., "Mobile Killer Applications In South Korea & Recommendations For U.S. Policymakers" (2003) 29 Brook. J. Int'l L. 239, and Mallat, N., "Theoretical Constructs of Mobile Payment Adopt-ion" at <<http://w3.msi.vxu.se/users/per/IRIS27/iris27-1100.pdf>> IRIS (Information systems research seminar in Scandinavia) conference paper no 27 Falkenberg, Sweden, 2004.

<sup>26</sup> Herzberg, A., "Payments and Banking with Mobile Personal Devices", *Communications of the ACM* (May 2003), Vol 46, Issue 5, at 53 – 58.

<sup>27</sup> Mallat, N., "Theoretical Constructs of Mobile Payment Adoption" at 4, *supra*, n 25. See for example Vodafone pre-paid system in "Vodafone M-Pay Bill Technical Pre Sales Pack" at <[http://online.vodafone.co.uk/dispatch/Portal/SimpleGetFileServlet?dDocName=BSA0044&revisions\\_electionMethod=latestReleased&inline=0&wt\\_oss=m-bill](http://online.vodafone.co.uk/dispatch/Portal/SimpleGetFileServlet?dDocName=BSA0044&revisions_electionMethod=latestReleased&inline=0&wt_oss=m-bill)> (19<sup>th</sup> June 2003). (Visited 6 April 2006).

Although various new payment methods were developed for the electronic commerce market, most of the time, the consumer still uses conventional electronic systems such as the EFT system, and the credit card for his electronic commerce transaction. In fact, visits to various internet commerce sites revealed that they are the major payment instruments accepted by the merchant.<sup>28</sup> The importance of the EFT payment and the credit card payment in the retail sectors is proved by a survey of ten countries' payment systems undertaken by the Bank for International Settlements in 2005.<sup>29</sup> Last but not least, an examination of several m-payment infrastructures also indicates their reliance on EFT and credit card payment.<sup>30</sup>

Considering the dominant place of the EFT and the credit card in the electronic commerce market, this research therefore focuses on loss allocation rules in the unauthorised credit card and EFT payment systems, particularly, the EFT payment via the debit card.

However, before analysing the loss allocation rules in the respective payment systems, it is necessary to describe the relationship between the parties involved in the payment transaction, in particular, between the consumer and the issuer. It

---

<sup>28</sup> See for example the growth of Visa debit card and credit card payment for the year 2003, not only in the conventional commerce but also in the internet commerce. Visa News Release, "Visa Global Debit Card Volume Surpasses Credit", at <http://www.corporate.visa.com/md/nr/press217.jsp>, (Visited 29<sup>th</sup> August 2005).

<sup>29</sup> Bank for International Settlement, Committee on Payment and Settlement Systems of the Group of Ten Countries, "Statistics on payment and settlement systems in selected countries", March 2005 at <http://www.bis.org/publ/cpss66.pdf>. See also Hayashi, F., *et al.*, A Guide to the ATM and Debit Card Industry, Federal Reserve Bank of Kansas City at <http://www.kc.frb.org/FRFS/ATMpaper.pdf> at 1, (Visited 16<sup>th</sup> April 2006).

<sup>30</sup> See for example, the mPark payment for parking spaces which incorporate a credit card payment at <https://www.mpark.com/mpark/memberReg.jsp>; PayPal Mobile payment at <https://www.paypal.com/cgi-bin/webscr?cmd=xpt/cps/mobile/MobileFAQ-outside>; DCMX mini<sup>TM</sup> offers by the NTT DoCoMo, Inc at <http://www.nttdocomo.com/pr/2006/001260.htmlVodafone-m-payment> and Osaifu-Keitai services also by NTT DoCoMo, Inc at <http://www.nttdocomo.co.jp/english/service/imode/osaifu/index.html> (Visited 26<sup>th</sup> April 2006).

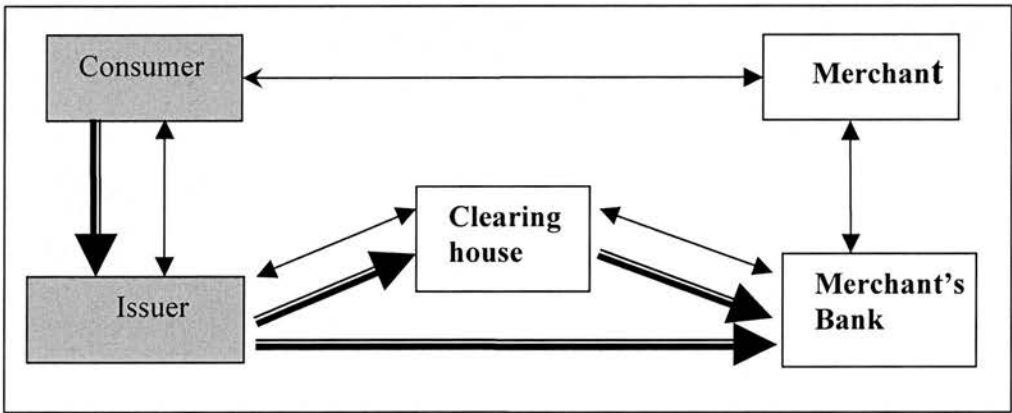
should also be mentioned that in some cases, the participants may also include a payment intermediary, a third party whose function is to convey the payment information between the consumer, the merchant and the issuer.

### 3 ELECTRONIC PAYMENT SYSTEMS AND THE PARTIES' RELATIONSHIPS

#### A Electronic Funds Transfer

Electronic payment via the EFT systems involves a web of inter-related yet, to a certain extent, independent relationships between two parties. To observe the flow of the EFT payment transactions the following diagram on the next page shows the working of the EFT system which involve the relationships between the consumer and his bank, the consumer and the merchant, the merchant and his bank, and between the banks in the relevant automated clearing house (the "ACH") network.

Diagram 1 EFT credit transaction flow<sup>31</sup>

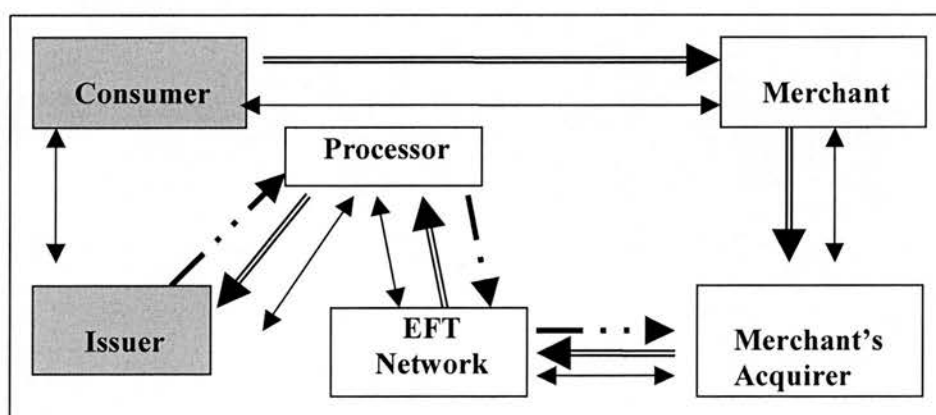


<sup>31</sup> Based on Figure 3.1 and the description of a credit transfer in Hooley, R. and Taylor, J., "Payment by Funds Transfer" in Brindle, M. and Cox, R., *Law of Bank Payments*, Chp 3, at 53.

Diagram 1. The thin arrows indicate the contractual relationships between the parties while the thick arrows show the flow of the payment information. Since the payment is a credit transfer payment, the payment transaction begins when the consumer instructs his bank to make a payment to the merchant. In this system the consumer must inform the issuer of the payee's details. If the issuer and the beneficiary banks are two different banks, the payment is cleared and settled via a clearing house. However, if the issuer and the beneficiary banks are one single entity or a branch of the other, the payment is cleared and settled within the bank's own system.

Apart from the credit payment, an EFT payment can also be made by a debit payment where the merchant, using the payment details supplied by the consumer, claims the payment from the issuer through the merchant acquirer.

Diagram 2 EFTPOS debit payment with Debit Card Transaction Flow<sup>32</sup>



<sup>32</sup> The diagram and the descriptions are based on Figure 2 and the descriptions given in the Boards of Governors of the Federal Reserve Systems Report to the Congress on the Disclosure of Point-of-Sale Debit Fees with modification at <http://www.federalreserve.gov/boarddocs/rptcongressposdebit004.pdf> (Visited 10<sup>th</sup> March 2006).

Diagram 2. In this diagram, the straight fine arrows show the contractual relationships between the parties in the debit transaction. The bold arrows show the flow of the payment information which the consumer transferred by swiping the card and entering the PIN into the merchant's system at the merchant terminal. The information is then transferred by the merchant's terminal that is connected to the merchant's acquirer, which then passes it to the EFT network. The information is sent to the issuer for authorisation, usually via a payment processor. After confirming the validity of the payment mandate by authenticating the PIN; and being satisfied that the card is not lost or stolen and that there are enough funds for the particular payment, the issuer sends a payment authorisation to the merchant's acquirer via the same parties as shown by the dotted arrows. At this stage, the issuer also debits the consumer's account. It should be noted that the issuer's and the merchant's accounts are settled via the clearing system.<sup>33</sup>

The debit card payment can be an off-line payment or online, depending on the method of authentication that is used. An online debit card payment allows the consumer to pay for his purchase almost instantaneously without the need to carry cash on his person, as long as the merchant's terminal accepts PIN authentication.<sup>34</sup> In other cases, the payment is made off-line, meaning that the consumer has to sign the sale draft as a mode of authorising the payment.<sup>35</sup>

---

<sup>33</sup> Supra n 31, Chp 3, Para 3-027–3-032.

<sup>34</sup> Bank for International Settlements, "Retail Payments in Selected Countries: A Comparative Study", (1999) at <<http://www.bis.org/publ/cpss33.pdf>> at 4-5. (Visited 12<sup>th</sup> April 2006).

<sup>35</sup> Ibid.



## B Credit Card Payment

Apart from EFT payment facilities, credit card payment is also popular among consumers.<sup>36</sup> This credit facility is offered in the form of a credit card, a charge card or a store card. Although both credit card and charge card provide identical credit facilities, they differ because a charge card holder is required to settle the credit in full at the end of each credit period while the credit card holder may pay the minimum amount of payment as specified by his monthly account statement.<sup>37</sup> While charge card and credit card are issued by a third party credit provider, a store card is usually issued by the merchant and its usage is limited within the merchant/issuer's own business or its chain of business.<sup>38</sup>

---

<sup>36</sup> At the end of fiscal year 2002, Visa reported a total of 1.2 billion cards issued by its worldwide membership, more than any other payment system. Visa Media Center, News Release, *San Francisco*, 18 December 2002, at <<http://corporate.visa.com/mc/press/press128.html>> (visited 5 March 2003).

<sup>37</sup> Smith, M. and Robertson, P., "Plastic Money", in Brindle, M. and Cox, R., *Law of Bank Payments*, Chp 4. See the history of the credit card in Rougeau, V. D., "Rediscovering Usury: An Argument for Legal Controls on Credit Card Interest Rates" (1996) 67 *U. Colo. L. Rev.* 1; Members of the Bankers Clearing House, *Payment Clearing Systems: Review of Organisation, Membership and Control* (1984) quoted in O'Mahony, D., *et al*, *Electronic Payment System* (1997) 11, Artech House, Inc.

<sup>38</sup> Ibid, M. Smith and P. Robertson, "Plastic Money", in Brindle, M. and Cox, R., *Law of Bank Payments*, Chp 4, Para 4-039.

The diagram illustrates the flow of a credit card transaction between six entities: Consumer, Merchant, Merchant's Acquirer, Issuer, Payment Processor, and Credit Card Network. The flow is as follows:

- Consumer** (shaded box) sends a payment request to the **Merchant** (white box) via a solid double-headed arrow.
- Merchant** sends the payment request to the **Merchant's Acquirer** (white box) via a solid double-headed arrow.
- Merchant's Acquirer** sends the payment request to the **Credit Card Network** (white box) via a solid double-headed arrow.
- Credit Card Network** sends the payment request to the **Payment Processor** (white box) via a solid double-headed arrow.
- Payment Processor** sends the payment request to the **Issuer** (shaded box) via a solid double-headed arrow.
- Issuer** sends the payment request back to the **Consumer** via a solid double-headed arrow.
- Issuer** also sends a dashed arrow to the **Consumer**.
- Merchant's Acquirer** sends a dashed arrow to the **Credit Card Network**.
- Payment Processor** sends a dashed arrow to the **Credit Card Network**.
- Credit Card Network** sends a dashed arrow to the **Payment Processor**.
- Credit Card Network** sends a dashed arrow to the **Merchant's Acquirer**.

To clear and settle the payment, the acquirer passes the payment slip to the issuer via the respective credit card network. At this stage, the network pays the acquirer the amount of the consumer payment minus the interchange fees. The network, in turn bills the card issuer for that payment. Finally, the issuer bills the consumer for the charges on a monthly basis.

26

In most cases, communication between the issuer and the network is done via a payment processor, a system through which the payment information has to pass before it reaches the credit card issuer.

### **C Internet-based and Mobile-based EFT and Credit Card Payment**

With the introduction of internet commerce and mobile commerce systems, various new payment systems were introduced to the consumer market. The new systems, to a certain extent, closely resemble the electronic payment systems that are already in the market except that they involve many new parties including, for instance, payment intermediaries, authenticating services and also mobile service providers.<sup>40</sup>

In so far as the EFTP and the credit card payments are concerned, there are two models of EFT and credit card systems for internet commerce. In the first model, the merchant's terminal captures the payment information and keeps it in its system for future use. When the consumer requests payment, the merchant's system directly transfers the information to its acquirer and to other parties for authorisation and settlement, similar to the process shown in Diagrams 2 and 3 above. This model is used, for instance, by the famous online bookstore Amazon.com.

The second internet payment model requires the service of a payment intermediary such as Paypal, WorlPay or Nochex. The intermediary takes the payment

---

<sup>40</sup> See Mallat, N., *et. al.*, "Mobile Banking Services", at 42-46, and Herzberg, A. "Payments and banking with mobile personal devices", at 53-58.

information and submits it to the consumer's bank for authorisation.<sup>41</sup> In the case of PayPal and Nochex, both companies act as the agents of the merchant and the consumer while in the case of WorldPay, it only provides a service to the merchant.<sup>42</sup>

Apparently, there is uncertainty as to the nature of the services provided by PayPal to the consumer. On the one hand, in the United States, PayPal acts as an "agent based upon (consumer's) direction and ... requests to use (its) Services..."<sup>43</sup> However, in the United Kingdom, the relationship is of an electronic money issuer and its customer by virtue of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001<sup>44</sup> which implements the EC Directive on the taking up, pursuit of and prudential supervision of the business of electronic money institutions.<sup>45</sup>

Although the function of PayPal is differently described in the United States and in the United Kingdom, in reality, in both jurisdictions, PayPal acts as an intermediary which undertakes to send the consumer's payment request to the issuer of the

---

<sup>41</sup> Paypal, at <<http://www.Paypal.com>>; WorldPay at <<http://www.worldpay.co.uk/>, and Nochex at <<http://help.nochex.com/?Action=Q&ID=106>> (Visited 28<sup>th</sup> December 2005).

<sup>42</sup> WorldPay merchant agreement at <[http://www.worldpay.com/about\\_us/index.php?page=tandc](http://www.worldpay.com/about_us/index.php?page=tandc)>, Nochex personal account agreement at <<http://help.nochex.com/messages/?Action=Q&ID=278>>, and merchant agreement at <<http://help.nochex.com/messages/?Action=Q&ID=271>>; and the PayPal user agreement at <<http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/ua-outside>> (10<sup>th</sup> April 2006).

<sup>43</sup> See clause 2 of the PayPal User Agreement at <<https://www.paypal.com/cgi-in/webscr?cmd=p/gen/ua/ua-outside>> (Visited 10<sup>th</sup> April 2006).

<sup>44</sup> See clause 2.1 of the PayPal User Agreement which applies to all European Union Countries except Germany, Austria, France, Italy, Spain, and Belgium at <<https://www.paypal.com/uk/cgi-bin/webscr?cmd=p/gen/ua/ua-outside>> (Visited 10<sup>th</sup> March 2006). SI 2001/544 as amended by the Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) Order 2001 SI 2001/3544 and the Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) Order 2002, SI 2002/682.

<sup>45</sup> Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions. OJ L 275 of 27 October 2000, p.39. See Part IV of the United Kingdom Financial Services and Markets Act 2000.

particular payment facilities on behalf of the consumer; it forwards the payment confirmation it received from the issuer via its merchant acquirer to the merchant and, pays the merchant the authorised payment.<sup>46</sup>

Diagram 4 illustrates an internet EFT or credit card payment made via the service of a payment intermediary.<sup>47</sup>

Diagram 4. Credit Card and EFTPOS Payment via an Intermediary<sup>48</sup>

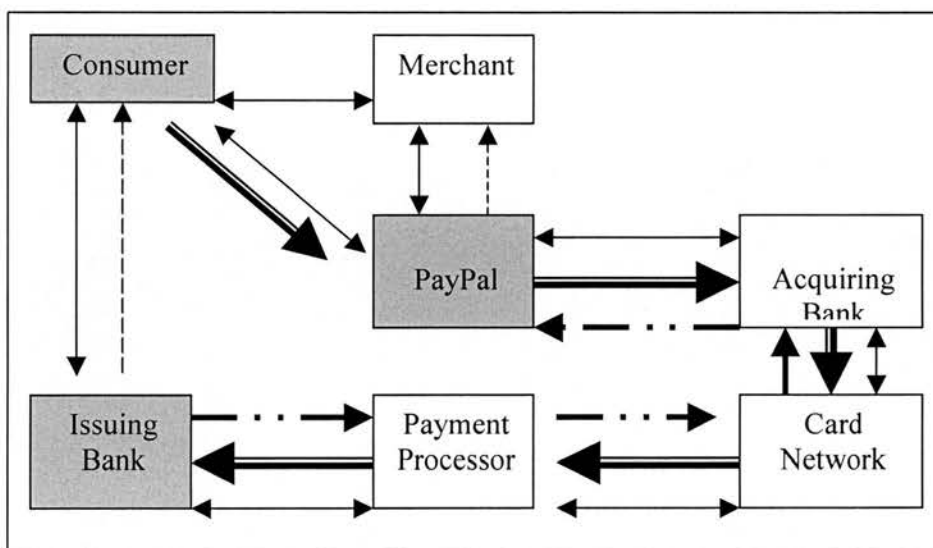


Diagram 4. In this diagram, the thin arrows indicate the contractual relationship between the parties. The bold dark arrows indicate the flow of the payment related information while the thin dotted arrows refer to the payment confirmation sent by

<sup>46</sup> See comments against the company being an electronic money issuer in González, A. G., "PayPal: the Legal Status of C2C Payment Systems" (2004) *Computer Law & Security Report* Vol. 20 Issue 4, 266, at 297-298.

<sup>47</sup> In Canada new Clearing Rules were introduced to regulate the clearing and settlement of online funds transfer payment. See Canadian Payments Association, Rule E2 Exchange for the Purpose of Clearing and Settlement Of Electronic On-Line Payment Items at <[http://www.cdnpay.ca/rules/pdfs\\_rules/rule\\_e2.pdf](http://www.cdnpay.ca/rules/pdfs_rules/rule_e2.pdf)> (Visited 10<sup>th</sup> April 2006).

<sup>48</sup> Based on a description in Technical Overview of PayPal as an Additional Payment Option at <[https://www.paypal.com/en\\_US/pdf/PP\\_Option\\_TechOverview.pdf](https://www.paypal.com/en_US/pdf/PP_Option_TechOverview.pdf)> (Visited 10<sup>th</sup> March 2006).

the issuer to the consumer and the merchant. In the case of the merchant, the notice was sent through the same communication channel that was used to transmit the payment authorisation. The heavy broken arrows indicate the flow of the payment authorisation.

In the internet payment made through PayPal as the intermediary, the information relating to the consumer's account, debit card details or credit card details are already in the PayPal's system. Therefore, when the consumer decides to make a purchase and proceeds to the merchant checkout, he is automatically taken to the PayPal website to initiate a payment request. At this stage, the consumer only has to enter the login (his e-mail address) and the PIN. Once PayPal confirms the identity of the consumer, it passes the payment request to the issuer, via its own merchant acquirer, through the credit card network and a processor, if there is one. The transaction flow from PayPal to the merchant acquirer and finally, to the issuer, is similar to the flow that takes place in the closed-network as shown in Diagrams 2 and 3 above, depending on the type of the payment chosen by the consumer. After receiving the payment authorisation, PayPal will send a confirmation notice to the merchant and a receipt of the payment to the consumer.<sup>49</sup>

A similar structure of the payment relationship applies to the m-payment systems. This structure is created by the involvement of a payment intermediary that may

---

<sup>49</sup> See details discussion in Kohlbach, M., "Making Sense of Electronic Money", (2004) 1 *The Journal of Information, Law and Technology* (JILT) at <[http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004\\_1/kohlbach/](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_1/kohlbach/)>. (Visited 10th March 2006).

include the mobile service provider or other independent payment intermediaries like PayPal.<sup>50</sup>

Diagram 5 shows an m-payment transaction using either a debit card or a credit card.

Diagram 5. M-Payment using credit card or debit card<sup>51</sup>

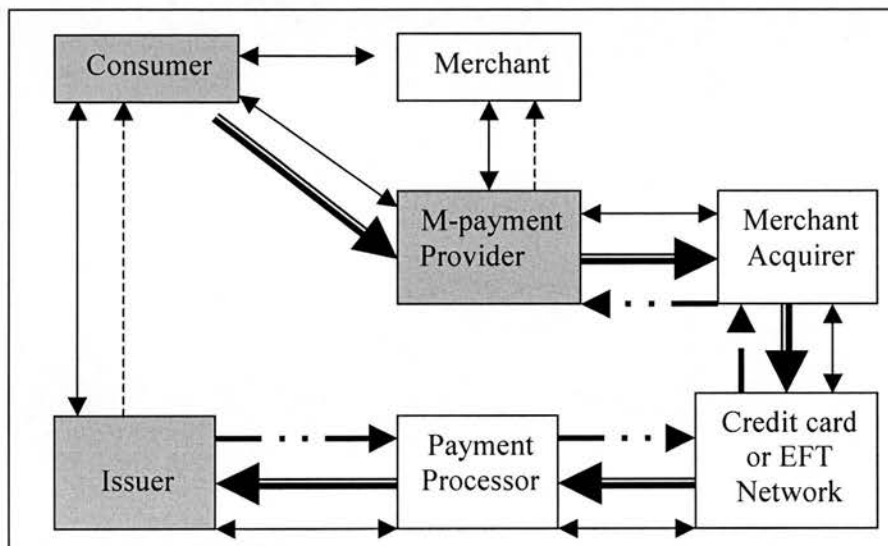


Diagram 5. In this diagram, the thin lines indicate the relationship between the parties. The bold arrows show the flow of the payment request by the consumer while the thick dotted arrows refer to the payment authorisation by the issuer. Finally, the thin dotted lines refer to payment confirmation notice sent by the issuer to the consumer and the merchant. In the case of the merchant, the notice is sent via the same channel through which the payment authorisation was sent.

<sup>50</sup> See for example PayPal mobile payment demo at <[https://www.paypal.com/en\\_US/m/mobile\\_demo.html](https://www.paypal.com/en_US/m/mobile_demo.html)>; McKitterick, D. and Dowling, J., "State of the Art Review of Mobile Payment Technology" at 10-15, at <<https://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-24.pdf>>; and "The Future Mobile Payments Infrastructure: A Common Platform for Secure M-Payments", Joint Project Feasibility Study by Institute for Communications Research <<http://www.itu.int/ITU-D/pdf/4597-13.3bis-en.pdf>> (Visited 10<sup>th</sup> April 2006).

<sup>51</sup> Based on the discussion in the references in note 50 above, with modification.

A consumer who wishes to make a payment through his mobile can use either an SMS text messaging model or a voice initiation model.<sup>52</sup> If he chooses the SMS text, he has to enter the product code and send the text to the shop code.<sup>53</sup> PayPal will call the consumer back to authenticate the order. By entering the PIN that was given to the consumer at the time of registration as an account holder, the consumer is authenticated. Thereafter, PayPal will repeat the purchase details for confirmation, which again can be confirmed by using the PIN. PayPal will send a notice of confirmation of the payment to the merchant and also the consumer. The process when the payment was initiated until the payment was confirmed follows the same route as in the credit card or EFT payment, depending on the type of payment card chosen by the consumer.

#### **4 THE LEGAL RELATIONSHIP OF THE CONSUMER AND THE ISSUER**

The previous diagrams revealed several linked, but in some circumstances independent, relationships between the parties in the payment systems. From these diagrams it is clear the consumer has contractual relationships with the issuer and also the merchant. Where the payment is intended for electronic payment through the internet or mobile systems, the consumer also has a contractual relationship with the payment intermediary.

---

<sup>52</sup> See the PayPal Mobile demonstration at <<https://www.paypal.com/cgi-bin/webscr?cmd=xpt/mobile/MobileOverview-outside>> (Visited 11<sup>th</sup> April 2006).

<sup>53</sup> See some of the merchants at <<https://www.paypal.com/cgi-bin/webscr?cmd=xpt/cps/mobile/T2offers-outside>> (Visited 12<sup>th</sup> April 2006).



The contractual relationship between the consumer and the issuer was described at length by Lord Atkin in *Joachimson v Swiss Bank Corp.*<sup>54</sup> Although the case was concerned with the cheque payment system, the description does, to a certain extent, applicable to the electronic payment systems.

In his Lordship's words, "I think that there is only one contract made between the bank and its customer. The terms of that contract involve obligations on both sides and require careful statement. They appear upon consideration to include the following provisions. The bank undertakes to receive money and to collect bills for its customer's account. The proceeds so received are not to be held in trust for the customer, but the bank borrows the proceeds and undertakes to repay them. The promise to repay is to repay at the branch of the bank where the account is kept, and during banking hours. It includes a promise to repay any part of the amount due against the written order of the customer addressed to the bank at the branch, and as such written orders may be outstanding in the ordinary course of business for two or three days, it is a term of the contract that the bank will not cease to do business with the customer except upon reasonable notice. The customer on his part undertakes to exercise reasonable care in executing his written orders so as not to mislead the bank or to facilitate forgery...."<sup>55</sup>

The above said contractual relationship places the consumer in the position of a principal and the issuer of the payment facility as an agent in paying the third

---

<sup>54</sup> [1921] 3 K.B. 110.

<sup>55</sup> Ibid, at 127.

parties.<sup>56</sup> The court in *Call v Ellenville Nat. Bank*<sup>57</sup> held that when a bank is collecting a cheque for its customer, it is an agent of the customer. The same principle applies in the relationship between the issuer of the electronic payment facility and the consumer since the consumer entered into the relationship with a firm understanding that the issuer can only debit his account with his mandate.

Because of the nature of their relationship, the issuer cannot make a payment from the consumer's account without his mandate. This law was summarised by Robert Goff J in *Barclays Bank Ltd v. W. J Simms Son & Cooke (Southern) Ltd*.<sup>58</sup> where he said that if the payment instruction was forged "[the issuer] pays without mandate from its customer; and unless the customer is able to and does ratify the payment, the bank cannot debit the customer's account... ." it was also said that when "the [issuer] has no mandate to pay, and acts with the mistaken belief that it has a mandate, then the [issuer] is paying as principal on its own behalf, and not on behalf of the customer."

The same rule applies in the electronic payment system. For instance, in *Mercedes Benz Finance v Clydesdale Bank*<sup>59</sup> it was held that the right to give an instruction to the bank to make payment from an account belongs to a person and remains with him, even if he had set up a direct debit transfer facility for the benefit of the payee.

---

<sup>56</sup> *Westminster Bank Ltd. v. Hilton* (1926) 43 T.L.R. 124, at 126. See Beale, H. G. *et. al.* (Eds), *Chitty on Contracts*, 29th Edn (2004) at 31-001 and 31-009, Sweet & Maxwell. (Hereafter Beale, H. G., *Chitty on Contracts*).

<sup>57</sup> 774 N.Y.S.2d 76, 78 (2004) *per* Slobod J.

<sup>58</sup> [1980] Q.B. 677.

<sup>59</sup> 1997 S.L.T. 905, at 909. The same legal relationship also exists as between the beneficiary bank and its customer. See *Hosni Tayeb v. HSBC Bank Plc* [2004] EWCH 1529.

Similarly, in *Barclays Bank plc v Quincecare Ltd*<sup>60</sup> it was said that “when the bank...acted on an order to transfer by immediate money transfer money from the Quincecare current account to Philip Evans & Co in Bournemouth, the bank was acting as Quincecare's agent.”<sup>61</sup> The same form of relationship was also found in the *Royal Products Ltd v Midland Bank Ltd*<sup>62</sup> where the court held that a funds transfer instruction sent by telex is an authority given by the customer to the bank, to transfer the money standing in credit to his account at that bank, to his account at another bank.

A similar form of relationship presumably exists between a credit card holder and the issuer. Millet J. noted in *Re Charge Card Services Ltd*,<sup>63</sup> that when the credit card issuer entered into a contract for the credit card payment facility, it was also acting as a principal in its own right and not merely as an agent for the accountholder.

The said contractual relationship prescribed upon the consumer and the issuer their rights and duties as an agent and a principal. The issuer's duties include a duty to make payment from the consumer's account according to the consumer's instruction. It was held in *Garnac Grain Co Inc v H M F Faure & Fairclough Ltd and another*<sup>64</sup> that if an issue is raised as to whether the agent had acted within his authority, it is necessary to ask: "what is it that the supposed agent is alleged to have done on behalf of the supposed principal?"<sup>65</sup>

---

<sup>60</sup> [1992] 4 All ER 363.

<sup>61</sup> *Barclays Bank plc v Quincecare Ltd and another*, at 375 – 376, per Steyn J.

<sup>62</sup> [1981] 2 Lloyd's Rep. 194, at 199, per Webster J.

<sup>63</sup> [1989] Ch 497, at 158.

<sup>64</sup> [1968] AC 1130.

<sup>65</sup> *Ibid*, at 1137, per Lord Pearson.

Similarly, the consumer also owes the issuer the duty to exercise care so as not to facilitate fraud. Finlay L J. said with respect to a cheque payment in *London Joint Stock Bank Ltd. v. Macmillan* <sup>66</sup> that “it is beyond dispute that the customer is bound to exercise reasonable care in drawing the cheque to prevent the banker being misled. If he draws the cheque in a manner which facilitates fraud, he is guilty of a breach of duty as between himself and the banker, and he will be responsible to the banker for any loss sustained by the banker as a natural and direct consequence of this breach of duty.” Therefore, if an unauthorised payment was facilitated by the consumer’s failure to exercise care the losses are the consumer’s.

From the review of the nature of the relationship between the consumer and the issuer, a framework for the allocation of fraudulent payment losses in the electronic payment systems can be outlined as follows:

First, the contractual relationship of an agent and a principal formed when the issuer agreed to provide an electronic payment facility to the consumer indicates that the allocation of an unauthorised payment should be based on the terms of their contract.

Second, because of the nature of their relationship, the allocation of any unauthorised payment should also be determined based on the question of whether the disputed payment was made by the issuer according to the consumer’s mandate.

---

<sup>66</sup> [1918] A.C. 777

Third, since the consumer owes the issuer the duty to exercise care to prevent unauthorised payment, the consumer's negligence also has an impact on the allocation of unauthorised payment losses.

Finally, having reached to this conclusion, it should however be clear that since an electronic payment systems are also governed by other specific electronic payment systems, it means that the allocation of the fraudulent payment losses may not only be based on the contract terms. In fact, the rules that govern the relationship between the consumer and the issuer of an electronic payment system may override the contract terms if the latter do not allocate the losses as prescribed by the regulations.<sup>67</sup> Hence, in some payment systems, negligence may not become the bases for the allocation of unauthorised payment losses. At the same time, some regulations may prescribe various precautionary actions which the consumer must do to avoid being negligent.

## **5 CONCLUSION**

This chapter described various retail electronic payment systems used by the consumer. The credit card and EFT payment by means of a debit card are widely used for purchases in the conventional electronic commerce systems via the EFTPOS system. They are also popular in the distance transaction through MOT or telephone shopping. Indeed, the use of the credit card and the debit card for distance

---

<sup>67</sup> See Chapter Introduction at page 7 to 9.

transaction, involving low and also high value purchase, is now a common phenomenon in internet commerce and also in the m-commerce market.

From the above discussions, it was also shown that the relationship between the consumer and the issuer, with regard to the payment made from the consumer's account, is one of agent and principal. Therefore, the relationship between the consumer and the issuer and their rights and liabilities are grounded in contract generally, and in contract of agency specifically. Because of the agency-based relationship, the payment mandate plays a very crucial role in assessing the validity of the payment made and charged by the issuer to the consumer's account.

**1 INTRODUCTION**

In the previous chapter, the relationship between the consumer and the issuer in the various electronic payment systems was described as that being of an agent and principal. It was also shown that in this type of relationship, the rights and liabilities of the parties, with regard to the payment made from the consumer's account, depends on the authority possessed by the issuer to make that payment.

In view of the above factors, this chapter will present an analysis of the method of issuing a payment mandate in electronic payment systems. It will also analyse the applicability of the particular loss allocation rules in assessing the validity of the respective mode of issuing the payment mandate.

**2 THE PAYMENT MANDATE AND THE MEANS OF ACCESS**

A mandate is generally a Roman form of gratuitous contract whereby a "mandant" requires a "mandatory" to act on his behalf.<sup>1</sup> However, a mandate is also defined as "a commission by which a party is entrusted to perform a service, especially without payment and with indemnity against loss by that party" and "a written authority enabling

---

<sup>1</sup>Zimmermann, R., *The Law of Obligations: Roman Foundations of the Civilian Tradition*, (1996), Chp 13, at 413-415, Oxford University Press and Macgregor, L. J., "Agency and Mandate" *The Law of Scotland, Stair Memorial Encyclopaedia* (reissued 2002) para 18 at 13. See *Copland v Brogan* 1916 S.L.T. 13, at 15.

someone to carry out transactions on another's bank account".<sup>2</sup> Apart from that, a mandate also refers to a relationship more like an agency where the agent receives fees for his service.<sup>3</sup>

In this dissertation, a mandate refers to the payment instruction given by the consumer to the issuer, authorising the latter to make a payment from the consumer's account. In *National Westminster Bank Ltd v Barclays Bank International Ltd*<sup>4</sup> and in *Barclays Bank Ltd v W.J. Simms Son & Cooke (Southern) Ltd*,<sup>5</sup> it was said that when the bankers paid money out of the customer's account within the given mandate, they acted in pursuant of their obligation to the customers and accordingly, had discharged the duty they owed to the customer.

Because of the importance of the mandate in the relationship between the issuer and the consumer, the contract between the consumer and the issuer usually, expressly or implied, describes the method of making and authenticating the payment mandate and also the effect of a fraudulent mandate.

In *London Joint Stock Bank v Macmillan*<sup>6</sup> it was concluded that "[a] cheque drawn by a customer is in point of law a mandate to the banker to pay the amount according to the tenor of the cheque". In this case, the clerk that worked with the respondents' firm

---

<sup>2</sup>Pearsall, J., *The Concise Oxford Dictionary*, 10<sup>th</sup> Edn. Revised (2001), at 865, BCA with arrangement with Oxford University Press BCA. (Hereafter Pearsall, J., *The Concise Oxford Dictionary*)

<sup>3</sup>Nicholas, B. N., *An Introduction to Roman Law* (1976) Reprinted 1987, at 188-189, Clarendon Press.

<sup>4</sup>[1975] Q.B. 654 at 666.

<sup>5</sup>[1980] Q.B. 677, at 679.

<sup>6</sup>[1918] A.C. 777, at 789, *per* Finlay L.C.



altered the sum of payment that was written down on the face of the cheque in the space for figures. The cheque did not contain the sum of payment in words. After the partners had signed the cheque, the clerk altered the amount of payment and the appellant paid the cheque accordingly. It was held that the firm had been guilty of a breach of the special duty arising from the relation of banker and customer to take care in the mode of drawing the cheque; that the alteration to the amount of the cheque was the direct result of that breach of duty; and that the bank was therefore, entitled to debit the firm's account with the full amount of the cheque.

The *London Joint Stock Bank's* case shows that it is necessary for the purpose of allocating the losses from a fraudulent payment to determine the presence of a mandate and also its validity. If the mandate is fraudulent, it generally means that the issuer is not entitled to debit the consumer's account, and the amount paid out of the consumer's account should be a loss to the issuer but not to the consumer.<sup>7</sup>

The form and the format of giving a mandate varies depending on the payment systems being used. The traditional method of making and authenticating the mandate in the paper-based payment system is a manuscript signature of the person initiating the payment.<sup>8</sup> Hence, in a cheque payment, a valid signature of the drawer on the face of the cheque confirms the authority of the bank to pay, according to the terms of the

---

<sup>7</sup> Cox, R. and Taylor, J., "Cheques" in Brindle, M. and Cox, R., *Law of Bank Payments* Chp 7, at 7-004

<sup>8</sup> Reed, C., "What is a Signature?" 2000 (3) *Journal of Information, Law and Technology* ("JILT"). at <<http://elj.warwick.ac.uk/jilt/00-3/reed.html>> (visited 30<sup>th</sup> April, 2002).

cheque.<sup>9</sup> Similarly, when an account holder uses a Giro Bank Transfer Form to make a payment, his signature authenticates the instruction given in the form and authorises his bank to transfer the funds accordingly.

In the electronic payment systems, either for electronic commerce or for high street transactions, the process of issuing the mandate involves a variety of technologies. If the payment is off-line, the processes rely on the use of the card; which sometimes bears a photograph, and the consumer's manuscript signature.<sup>10</sup> However, if the payment is made at the merchant's terminal and the system is online, the mandate issuance and the authentication require the payment card and the PIN.<sup>11</sup> Where electronic payments are for the internet or m-commerce, the mandate usually requires the consumer to type in the card or the account details at the initial stage of registering as an account holder. In subsequent transactions, the mandate is issued using the PIN that was given to him at the time he registered as the account holder.

As the methods for the issuance of the mandate are diverse, the loss allocation scheme in a particular type of payment system must contain rules that can be applied to assess the validity of the payment mandate issued with the use of these methods. If the rules are limited in scope and applicable only to some of the methods of issuing the mandate, they

---

<sup>9</sup>*London Joint Stock Bank, Limited Appellants; v. Macmillan and Arthur Respondents* [1918] AC 777.

<sup>10</sup> See for example the definition of and identification method which is used to authenticate payment in the Federal Reserve Board (the "FRB") Staff Interpretation to s. 205.6(a) of Reg. E.

<sup>11</sup> Smith, M. and Robertson, P., "Plastic Money" in Brindle, M. and Cox, R., *Law of Bank Payments*, Chp 4, Para 4-027. Nowadays in almost every region the credit card and the debit card are being upgraded to PIN based authentication. See in the United Kingdom alone there were around 107 millions of PIN based card issued by the end of June 2005. See the APACS Press Release 29<sup>th</sup> July 2005 at <<http://www.apacs.org.uk/>> (Visited 29<sup>th</sup> August 2005).

may affect the protection of the consumer. That is so because the loophole gives the issuer the opportunity to use its own loss allocation rules, which may be unfair on the consumer, to assess the validity of the payment mandate and to allocate the losses accordingly.

### **3 THE PAYMENT MANDATE AND THE LOSS ALLOCATION RULES IN THE UNITED STATES**

#### **A The Scope of Unauthorised Payment Mandate in the TILA**

Section 103 (o) of the TILA describes an unauthorised credit card payment as a payment initiated by unauthorised use of the credit card.<sup>12</sup> In *Mastercard, Consumer Credit Div. of First Wisconsin Nat. Bank of Milwaukee v Town of Newport*,<sup>13</sup> the court highlighted that "unauthorized use," under s.103 (o) of the TILA refers to "the use of a credit card by a person other than the card holder."

The above definition of unauthorised credit card usage points to two aspects of the rule. The first component refers to the circumstances when unauthorised credit card payment occurs and the second part refers to the mode used by the fraudster to issue a fraudulent mandate and consequently resulted in an unauthorised payment.

---

<sup>12</sup> See also s. 226.12(b)(1) of Reg. Z.

<sup>13</sup> 133 Wis.2d 328, 396 N.W.2d 345 Wis.App.,1986, at 347. *Martin v. American Express, Inc.* 361 So.2d 597 Ala. Civ. App. 1978, at 600-601 and *Towers World Airways Inc. v. PHH Aviation Systems Inc. and PHH Group Inc.* 933 F.2d 174, 179 C.A.2 (N.Y.),1991.

It should be noted that the definition of unauthorised credit card payment in s 103 of the TILA does not provide the detailed circumstances in which the payment may occur, except by referent to unauthorised use of the card. Thus, it becomes a necessity to analyse the TILA provisions to identify the circumstances when the credit card usage is unauthorised.

The first provision is s. 133 (a) (1) (D) which provides that a consumer's liability is capped at a maximum of \$50 if he notified the issuer of "loss and theft" of the card.<sup>14</sup> This rule suggested that unauthorised use occurs only when the credit card is lost or stolen. Section 133 (a) (1) (E), however, suggests a wider scope of unauthorised use. It requires the consumer to notify the issuer of "unauthori[s]ed use that has occurred or may occur as a result of loss, theft or otherwise". Reading these two subsections together, it appears that the situation where unauthorised credit card usage may occur is not limited to the case of a lost or stolen card.<sup>15</sup>

Nevertheless, note that s. 133 (a) (1) did not explain the circumstances that fall under the scope of "otherwise". Accordingly, it becomes necessary to refer to the judicial interpretation of the rule in order to define the scope of unauthorised credit card use other than the loss or theft of the card. In this regard, the decisions in *Martin v. American Express, Inc.*<sup>16</sup> and *Towers World Airways Inc. v. PHH Aviation Systems Inc.*

---

<sup>14</sup> Section 133 (a)(1)(D)

<sup>15</sup> Clark, S. C., "*Walker Bank & Trust Co. v Jones*: New Meaning for the Phrase 'Don't Leave without It'" (1984) *Utah L. Rev.* 865, at 880

<sup>16</sup> 361 So.2d 597 Ala. Civ. App. 1978, at 600-601.

*and PHH Group Inc.*<sup>17</sup> are of great assistance. In *Martin* the court explained that “[section 133(a)] clearly indicates that . . . protection under the TILA is warranted where the card is obtained from the card holder as a result of loss, theft, or wrongdoing”. On the other hand, the court in *Tower* stressed that, “[t]hough the card holder's relinquishment of possession may create in another the appearance of authority to use the card, the statute clearly precludes a finding of apparent authority where the transfer of the card was without the card holder's consent, as in cases involving theft, loss, or fraud.”<sup>18</sup> It further said, that the Congressional intent of the 1970 amendment to the TILA demonstrates that only cases of involuntary card transfers fall under the scope of unauthorised use in s. 103(o) and s. 133(a) of the TILA.<sup>19</sup>

These decisions show that unauthorised credit card payment occurs when the credit card falls into the hand of the user as a result of loss, theft, fraud or any wrongdoing which constituted a non-voluntary transfer of the card.

However, this scope of unauthorised credit card payment refers to only one mode of accessing the consumer's account, namely, by using the credit card. This definition leads to a conclusion that if the credit card payment mandate is issued using the credit card, the TILA rules are applicable in litigating the dispute but not when the mandate is issued with the use of other access modes. This finding can also be supported by the definition of the credit card in s. 103(k) of the TILA and s.226.2 (a)(15) of Reg. Z,

---

<sup>17</sup> 933 F.2d 174, C.A.2 (N.Y.),1991.

<sup>18</sup> *Ibid*, at 177.

<sup>19</sup> *Ibid*.

which described a credit card to include “other credit device existing for the purpose of obtaining money, property, labor or services on credit.” A device generally means “something that is formed or formulated by design and usually with consideration of possible alternatives, experiment, and testing: something devised or contrived”.<sup>20</sup> It can also mean a contrivance, mechanism, machine, machinery, utensil, apparatus, etc<sup>21</sup>. Thus, the “device” in s. 103(k) of the TILA and s.226.2 (a) (15) of Reg. Z. connotes the use of a tangible access mode which exclude credit card number and details.

Regardless of the above argument, the “device” may also be used to refer to a method of accessing the account, regardless of its form. This definition is used in s. 1029 (e) (1) of the Credit Card Fraud Act<sup>22</sup>; a statute which regulate criminal use of credit card, to include credit card numbers.<sup>23</sup> Nevertheless, it is not clear whether this definition can be used to define the rule in s. 133 of the TILA. Although it was held in *Bragdon v. Abbott*,<sup>24</sup> that the interpretation of a statute may be used to interpret the same word used in another statute, it however specifically pointed to using the interpretation of an earlier statute to interpret a later statute. Since the TILA was passed before the Credit Card

---

<sup>20</sup> Webster's Third New International Dictionary 1402 (2002).

<sup>21</sup> Tulloch, S., *Reader's Digest Oxford Wordfinder* (1996) Oxford University Press.

<sup>22</sup> Credit Card Fraud Act of 1984.

<sup>23</sup> *United States v. Yellowe* 24 F.3d 1110 C.A.9 (Hawai'i),1994 and *United States v. Klopff*, 2005 U.S. App. LEXIS 19246 Section 1029 (e)(1) “the term “access device” means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).”

<sup>24</sup> 524 U.S. 624, 645, 118 S. Ct. 2196, 141 L. Ed. 2d 540 (1998). “When administrative and judicial interpretations have settled the meaning of an existing statutory provision, repetition of the same language in a new statute indicates, as a general matter, the intent to incorporate its administrative and judicial interpretations as well”.

Fraud Act it seems that the problem cannot be settled by referring to *Brandon*. Moreover, the word “device” was specifically defined by the Credit Card Fraud Act and not by the administrator or the judiciary. Hence, it can be argued that the definition of the word “device” in the Credit Card Fraud Act cannot be used to define the same word in s. 133 of the TILA.<sup>25</sup>

Another approach to determine the mode of access that falls within the TILA loss allocation scheme is to examine the reference to the verb “use” in the description of unauthorised payment as “unauthorized use”. However, this interpretation may result in two scopes of unauthorised credit card payment. The first is a narrow scope, based on the literal interpretation of the word “use”. The second is a liberal scope of the rules to be interpreted, based on the purpose of the TILA, which includes the protection of the consumer against unfair credit card practices; which may include excessive liabilities.<sup>26</sup>

Literally,<sup>27</sup> the word “use” refers to active employment of the subject of use, in this case the credit card, as an “operative factor” in the commission of a particular action.<sup>28</sup> Hence, the card itself must be used to issue the payment mandate before the mandate can

---

<sup>25</sup> Kruk, T. L., “What constitutes violation of 18 U.S.C.A. §1029, prohibiting fraud or related activity in connection with credit card or other credit access device, (2005) 115 *A. L. R. Fed.* 13.

<sup>26</sup> Section 102 (a) of the TILA. See Leming, T. *et. al.*, “Purpose, construction, and application” 17 *Am. Jur.* 2d, Consumer Protection § 3,. See the case of *Mourning v. Family Publications Service, Inc.*, 411 U.S. 356, 93 S. Ct. 1652, 36 L. Ed. 2d 318 (1973) and *Stieger v. Chevy Chase Sav. Bank, F.S.B.* 666 A.2d 479, 485, D.C., 1995.

<sup>27</sup> It is said that in interpreting a statute, the court must begin by examining the plain meaning of the statutory language. *K Mart v. Cartier, Inc.*, 486 U.S. 281, 108 S.Ct. 1811, 100 L.Ed.2d 313 (1998). Moreover, where the statute is remedial and designed to protect a certain class of persons, in the TILA case the consumer, it should be construed liberally in favour of the consumer. *Smith v Fidelity Consumer Discount Co.*, 898 F.2d 896, 898 (3d Cir. 1990).

<sup>28</sup> *U.S. v. Hall* 110 F.3d 1155, 1160, C.A.5 (Miss.), 1997.

be validated or invalidated according to the TILA rules. This definition excludes a payment mandate issued with the use of other means such as the credit card number from the TILA loss allocation scheme.

The narrow scope of the rule renders ineffective s.133 (c), which prevents the issuer from contracting out of the TILA,<sup>29</sup> and s. 133 (d), which made the TILA loss allocation rules the exclusive rules to be applied in allocating unauthorised credit card payment<sup>30</sup> because it gives the issuer the opportunity to use its own loss allocation rules to determine the validity of the mandate issued without using the credit card.

Eventually, a restricted interpretation of the TILA loss allocation rules would also render the whole TILA loss allocation scheme inapplicable to a payment mandate issued without using the card, because all the rules in the TILA loss allocation scheme refer to “unauthorized use” of the card.<sup>31</sup>

A restricted scope of unauthorised credit card payment also affects the protection of the consumer in the internet or the m-payment systems, where the payment mandate is usually issued by typing in the card details.

---

<sup>29</sup> Section 133 (c) “Nothing in this section imposes liability upon a card holder for the unauthorized use of a credit card in excess of his liability for such use under other applicable law or under any agreement with the card issuer”

<sup>30</sup> Section 133 (d) “Except as provided in this section, a card holder incurs no liability from the unauthorized use of a credit card.”

<sup>31</sup> See s.133 of the TILA.



However, a liberal interpretation of the TILA loss allocation rules, taking into account the purpose of the TILA, should be explored to determine whether the TILA loss allocation rule may be applied to assess the validity of a payment mandate issued with the use of the card details.<sup>32</sup> Numerous judicial decisions show that the TILA loss allocation rules were enacted for the protection of the consumer and accordingly, it should be construed liberally in favour of the consumer.<sup>33</sup>

A liberal interpretation of “unauthorized use” of the credit card was applied by the court in the case of *Carrier v. Citibank (South Dakota)*.<sup>34</sup> In this case, a dispute arose over a series of credit card payments made by an employee who used, in some instances, her employer’s credit card numbers and, in others, the employer’s secondary credit card. Despite the different methods used by the employee to issue the payment mandates, the court did not differentiate the payments made using the card numbers and those made using the card. Instead, all the losses were allocated to the credit card account holder because the card user possessed an apparent authority to make the payments at the time of the transactions.

---

<sup>32</sup> In *Cabell v. Markham*, 148 F.2d 737 (2d Cir.1945), the purposive approach to statutory interpretation was explained: “Of course it is true that the words used, even in their literal sense, are the primary, and ordinarily the most reliable, source of interpreting the meaning of any writing: be it a statute, a contract, or anything else. But it is one of the surest indexes of a mature and developed jurisprudence not to make a fortress out of the dictionary; but to remember that statutes always have some purpose or object to accomplish, whose sympathetic and imaginative discovery is the surest guide to their meaning.

<sup>33</sup> *Pfennig v. Household Credit Services, Inc.* 295 F.3d 522, 525, C.A.6 (Ohio), 2002, *Abel v. KeyBank USA, N.A.*, 2003 U.S. Dist. LEXIS 27175 (N.D. Ohio, Sept. 24, 2003) and *Short v. Wells Fargo Bank Minn., N.A.*, 401 F. Supp. 2d 549, 2005 U.S. Dist. LEXIS 28612 (S.D. W. Va., 2005).

<sup>34</sup> N.A. F.Supp.2d, 2005 WL 2002484 D.Conn.,2005.

Although the court, in this case, did not define “unauthorized use” from the perspective of the credit card or the card details, its indifference to the disputed payments initiated, using the different methods, indicates that the TILA loss allocation rules should also be used to assess the validity of a payment mandate issued with the use of the consumer’s card details.

Based on the above discussion, it can be concluded that unauthorised credit card payment refers to payment made with the use of a consumer’s credit card, which was obtained by a fraudster as a result of loss or theft or any form of involuntary transfer. Indeed, if the liberal interpretation is accepted, unauthorised payment under the TILA may also refer to payment made using the card details obtained by wrongful means.<sup>35</sup>

## **B      The Scope of the Payment Mandate in the EFTA**

The EFTA, like the TILA, also refers to unauthorised payment as payment initiated by a person without authority.<sup>36</sup> This description of unauthorised payment is believed to refer to cases where the person who initiated the payment came into possession of the mode of access to the consumer’s account by wrongdoing. However, compared to the TILA, the definition of unauthorised EFT payment refers to a broad range of methods of issuing a payment mandate, namely, the “card, code or means of access”. In fact, s.

---

<sup>35</sup> See above at 49-50.

<sup>36</sup> Section 903 (11).

205.2 (a) (1) of Reg. E also shows that the mandate may be issued, not only by using the individual mode of access, but also a combination of them.

Based on these provisions, it is clear that when a dispute arises as to the validity of an EFT payment, the EFTA rules must be applied to assess the validity of the payment mandate if the mandate was issued using the card, code or a combination of the card and the code.

However, the rules do not stop at naming the access mode. Indeed, they also refer to “other means of access”, which is a functional way of describing the method to access the consumer’s account. This definition makes the EFTA rules more flexible and adaptable to the changes that happen and will occur in the payment systems’ technology. Moreover, the definition of an “electronic funds transfer” as a system in which the payment instruction was given to the issuer via “an electronic terminal, telephonic instrument, or computer or magnetic tape which does not necessarily require the use of a debit card, also supports a wider scope of the EFTA mode of issuing a payment mandate.<sup>37</sup>

The application of this rule can be seen in the case of *Ognibene v Citibank, N.A.*<sup>38</sup> Ognibene claimed that the ATM transaction debited to his account was unauthorised. In fact, the transaction was effected by the use of his card, which he voluntarily gave to

---

<sup>37</sup> See s. 903 (6) of the EFTA, and s. 205.3 (b) and s.205.2 (h) of Reg. E.

<sup>38</sup> 112 Misc.2d 219, 446 N.Y.S.2d 845, (1981) at 847.

the user, in combination with the PIN, which the user obtained by illegally observing Ognibene at the ATM machine. It was decided that the whole losses were the issuer's losses because the method of giving the payment mandate was partially obtained by involuntary transfer.

The Ognibene decision showed that since access to the ATM machine required a combination of the card and the PIN, by voluntarily giving only the card to the fraudster, the consumer did not give the fraudster the means of access to his account. As a result the payment mandate issued with the use of the card and the PIN became an invalid mandate, which the issuer could not rely on.

This case clearly expanded the scope of the payment mandate which falls within the EFT loss allocation scheme. Instead of restricting the rules to apply to a certain mode of issuing a payment mandate, the case shows that a payment mandate can be issued with the use of any mode of access. In fact, this case also shows that if the system where the EFT payment is made requires a combined mode of access in order to issue a payment mandate, the validity of that mandate must be assessed according to the EFTA loss allocation rules.

A functional approach to the definition of an unauthorised EFT payment protects the consumer when a fraudulent payment is made by the issuer upon receiving a fraudulent mandate, irrespective of the mode chosen by the fraudster to issue the mandate. Therefore, a fraudulent mandate may be issued using a debit card, or the card details, or

a combination of the card and the PIN or even the account numbers, yet its validity is still assessed based on the EFTA rules. In fact, the court in *Kashanchi v. Texas Commerce Medical Bank, N.A.*<sup>39</sup> stressed that the EFTA defined electronic funds transfer in broad and general terms to give the Board the flexibility to determine the applicability of the EFTA rules to “new or developing electronic services”.

The functional interpretation of an unauthorised EFT payment would prevent the issuer from allocating the losses caused by a fraudulent internet or m-mobile EFT payment except by following the EFTA loss allocation scheme. Indeed, the functional approach to the definition of an unauthorised EFT payment would also give effect to the rule in s. 909(d) and (e) of the EFTA loss allocation rules. These provisions clearly stress that the EFTA loss allocation rules provide the minimum consumer protection scheme which the issuer must apply in allocating an unauthorised EFT payment. However, if the EFTA rules only cover an EFT payment initiated with the use of a debit card, the consumer may be subjected to the issuer’s contractual loss allocation rules, which differ from the EFTA rules, when the payment is initiated with the use of other access modes. This restricted interpretation would contradict the purpose of the EFTA.<sup>40</sup>

The above discussions reveal that the TILA loss allocation rules are applicable in assessing the validity of a payment mandate issued using a credit card. It was also

---

<sup>39</sup> 703 F.2d 936, 940, C.A.Tex.,1983

<sup>40</sup> Section 902 (b) “It is the purpose of this title to provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems. The primary objective of this title, however, is the provision of individual consumer rights.”

explained that by applying the purposive interpretation to the language of s. 133 of the TILA, the validity of a payment mandate issued with the credit card details can also be assessed, according to the TILA loss allocation rules.

On the other hand, the EFTA loss allocation rules do not require a purposive interpretation in order to bring the mandate issued using the card details or any other mode of assessing the consumer's account within its loss allocation scheme.

#### **4 THE PAYMENT MANDATE AND THE LOSS ALLOCATION RULES IN THE CCA, THE BANKING CODE AND THE DSRs IN THE UNITED KINGDOM**

##### **A The Scope of the Payment Mandate in the CCA and the DSRs**

In the United Kingdom, the CCA also assesses the validity of the payment mandate by linking it to the method of gaining access to the credit card account. Section 84(1) of the CCA limits the consumer's liability for losses caused by the unauthorised use of his credit card "when the [credit card] ceases to be in the possession of any authorised person and ending when the [credit card] is once more in the possession of an authorised person".<sup>41</sup> According to s. 84(3), the issuer cannot allocate the losses to the consumer if the losses occurred after a notification of "loss, theft or possible misuse of the credit

---

<sup>41</sup> Section 84(1) of the CCA. See Goode, R. M., *Consumer Credit Law and Practice* (1999) Issue 6 Para 5.10 and 5.20, Butterworths. (Hereafter Goode, R. M., *Consumer Credit Law and Practice*).

card” was given to the issuer.<sup>42</sup> Nevertheless, s. 84(2) of the CCA allowed the issuer to allocate any amount of losses to the consumer if the user “acquired possession [of the card] with the debtor’s consent.”

From these three provisions, a number of rules can be deduced to explain the scope of the payment mandate which is governed by the CCA loss allocation rules.

The first rule is that under the CCA loss allocation rules, the responsibility of the consumer for the credit card payment involves an assessment of the validity of the mandate issued with the use of the credit card. Such a conclusion is to be drawn from the language of s. 84 (1) – (3A) of the CCA which refers to “the use of the credit token”. As the word “use” literally means “to employ to any purpose”,<sup>43</sup> it is believed that the CCA provision which reads “the use of the credit token” implies the use of the credit card to issue a payment mandate. Hence, it can be deduced that the CCA loss allocation rules in s. 84 (1) to (3A) can only be used to assess the validity of the credit card payment mandate when the mandate was issued by using the credit card but not in other cases.

It is generally known that a credit card payment can be initiated, even without using the card. Accordingly, if the above interpretation is applied to the CCA loss allocation scheme, it is questionable whether the scheme can be extended to cover the payment

---

<sup>42</sup> Section 84(3) of the CCA.

<sup>43</sup> *British Motor Syndicate, Ltd. v. Taylor & Son* [1900] 1 Ch. 577, at 583.

mandate issued using a method other than the card. In particular, can the issuer determine the validity of the payment mandate issued using the card details with its own loss allocation rules or must it apply the CCA loss allocation rules?

Apparently, a strict literal interpretation of the phrase “use of credit token” mentioned earlier would not bring the mandate issued using the card details under the CCA scheme.

It should be noted that this interpretation is prejudicial to the consumer because it defeats the effect of s.173 (1) and (2) of the CCA which prohibits contracting out of the CCA scheme. According to these provisions, any of the issuer’s contract terms that are inconsistent with the CCA consumer protection scheme, including the duty and liability of the consumer card holder, are void. Now, since the literal interpretation puts the payment mandate issued using the card details outside the CCA loss allocation regime, the issuer may use its own rules to determine the validity of the mandate, and eventually allocate the losses based on that assessment.

Therefore, in the interests of the consumer, and to give effect to s. 173, it is believed that the word “use” should be liberally interpreted to refer to the mean of gaining access to the consumer’s account, which includes the card details.<sup>44</sup>

The uncertainty with respect to the scope of the payment mandate under the CCA has now been settled with the passing of the DSRs in 2000.<sup>45</sup> Regulation 21 of the DSRs

---

<sup>44</sup> *Eaton Baker and Another Appellants v. The Queen Respondent*, [1975] A.C. 774, Privy Council.



read together with s. 84 (3A), as amended by Reg. 21(5), provides that the consumer is not responsible for an unauthorised credit card payment made in a distance transaction if the person who initiated the payment was not authorised to do so by the consumer. Although Reg. 21 also refers to “fraudulent use” of a payment card, the definition of a distance contract, which refers to contracting via a distance communication system,<sup>46</sup> shows that the payment mandate under the CCA loss allocation rules can be issued using either the card or the card details, or any other mode of access that is compatible with the distance communication system.

Accordingly, it can be concluded that in so far as a credit card payment is concerned, the payment mandate that is governed by the CCA loss allocation scheme, as amended by the DSRs, can be issued either using a credit card or the card details.

## **B The Scope of the Payment Mandate in the Banking Code**

Another loss allocation scheme that is applicable in the United Kingdom is the Banking Code (the “Code”). The Code scheme applies to debit card and charge card payments which are outside the CCA loss allocation regime. The Code also applies, to a certain extent, to credit cards but not store cards, provided the Code rules do not contradict the CCA.<sup>47</sup>

---

<sup>45</sup> SI 2000/2334.

<sup>46</sup> Regulation 3 (1) and Sch. 1.

<sup>47</sup> The CCA loss allocation rules only apply to credit token which definition excludes the debit card unless the debit card is used to incur overdraft. See the Ombudsman decision March 2001 at

The Code loss allocation rules cover a wider scope of a payment mandate as evidenced by the rule in s. 12.12. The first proviso of the rule requires the consumer to inform the issuer of the loss or theft of his card or that his PIN is known by another individual. From this rule it can be deduced that the payment mandate that is governed by the Code includes a mandate issued using the card. The Ombudsman in the case of a Miss L, which involved a cheque guarantee card, applied the Code loss allocation rules to determine the validity of a payment mandate issued by a joint account holder who was in possession of the card.<sup>48</sup>

Apart from that, the reference to the PIN, which is to be used to initiate payment at the point of sale terminal or to access the account at the ATM machine,<sup>49</sup> also shows that the mandate issued by using the card and the PIN also falls within the scope of the Code loss allocation rules. Accordingly, if a dispute arises as to the validity of a payment made by the issuer upon receiving a mandate issued using these modes, the Code rules should be applied by the issuer, unless the dispute involves a credit card where the CCA prevails over some of the Code rules.

---

*<<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/3/plastic-cards.htm>>* (Visited 6<sup>th</sup> June 2005). Similarly the rules are not applicable to the charge card which is exempted by virtue of s. 16 (5)(a) of the CCA and also art. 3 (1) (a) (ii) of the Consumer Credit (Exempt Agreements) Order 1989, SI 1989/869. See the Code's Glossary definition of card as to, "includes debit, credit, cheque guarantee, charge cards and cash cards."

<sup>48</sup> The Ombudsman News March 2001, at *<<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/3/mandates.htm>>* (Visited 12 April 2006).

<sup>49</sup> The Code's Glossary defined PIN as "[a] confidential number which allows customers to buy things, withdraw cash and use other services at a cash machine. You will often have to enter your PIN into a point of sale terminal, instead of signing a receipt, to authorise a transaction.

The applicability of the Code rules to determine the validity of a mandate issued with a combined use of card and PIN was applied by the Ombudsman in many cases including the case of a Mr H, involving a theft of a wallet. The Ombudsman found that because Mr H had kept the PIN together with the card in his wallet, the issuer was entitled to debit his account with the amount of withdrawal requested by the fraudster.<sup>50</sup>

The second and the third provisions of s. 12.12 show that the Code loss allocation rules should also be applied by the issuer in a dispute over the validity of a payment mandate issued using the card details. These rules incorporated Reg. 21 of the DSRs which is applicable to a debit card and also a charge card.<sup>51</sup>

Based on the above discussion, it is clear that the CCA and the Banking Code loss allocation rules as supplemented by the DSRs, are applicable in assessing the validity of the payment mandate issued using the card or the card details. The Banking Code, in fact, covers the mandate issued with the use of the card and the PIN. Moreover, the Code is applicable to the credit card payment as long as it does not contradict the CCA; while the CCA does not contain a rule which refers to the use of the card and the PIN, the validity of a payment mandate issued using the credit card and the PIN should also be assessed, according to the Code rules.

---

<sup>50</sup> The Ombudsman News September 2001, at <<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/9/sept-disputed-cash-machine-withdrawals.htm>> (Visited 12<sup>th</sup> April 2006).

<sup>51</sup> Regulation 21 (6) of the DSRs.

## 5 THE PAYMENT MANDATE AND THE LOSS ALLOCATION RULES IN THE MALAYSIAN CC GUIDELINES AND EFT GUIDELINES

### A The Scope of the Payment Mandate in the CC Guidelines.

Paragraph 13 of the CC Guidelines refers to “unauthorised payment” as a payment which was made “as a consequence of a lost or stolen credit card”. Literally “consequence” means “a result or effect”.<sup>52</sup> On the other hand, “result” as a noun refers to an “outcome” while as a verb it means to “occur or follow as a result”.<sup>53</sup> Accordingly, “consequence” can be interpreted to refer to something or some events that happened as a result of certain actions or certain circumstances.<sup>54</sup> In the case of Para 13.2 of the CC Guidelines, the event is the unauthorised credit card transaction that follows the loss or theft of the credit card.

Based on a literal interpretation of Para 13.2, it is believed that only a payment mandate issued using a credit card falls within the CC Guidelines loss allocation scheme. However, it should be noted that since the same rule did not specifically refer to the “use” of the card like the TILA and the CCA, it is also possible to interpret the rule in Para 13.2 in a wider way so that it also applies to the payment mandate issued with the use of the credit card details. Moreover, because of the word “consequence”, it can be

---

<sup>52</sup> Pearsall, J., *The Concise Oxford Dictionary*, at 303.

<sup>53</sup> *Ibid*, at 1221.

<sup>54</sup> Referred to based on the principle of persuasive authority to the Singapore case of *Singatronics Ltd v Insurance Co of North America* [1994] 1 SLR 500, at 511.

argued that the details obtained from a stolen or a lost card is a as “consequence” of those two events. Thus, the payment mandate issued using the details obtained from the respective card must be assessed according to the CC Guidelines loss allocation rules.<sup>55</sup> Nevertheless, this is an unconfirmed suggestion since the interpretation of the rule is something unknown to the public, as the Mediator’s decision has not been published publicly.

## **B The Scope of the Payment Mandate in the EFT Guidelines**

The EFT Guidelines provide a scheme for allocating the losses caused by a fraudulent EFT payment. However, its definition of an unauthorised EFT payment does not explain, clearly or implicitly, the types of mandate which are governed by its loss allocation rules. Therefore, it is necessary to thoroughly search the EFT Guidelines to find the scope of an EFT payment mandate so that its validity can be assessed according to the Guidelines loss allocation rules.

The first are the notification rules in Para 15 (3) and Para 16 which require the consumer to inform the issuer of the “stolen, lost, or misused debit card” or breach of the access code confidentiality. This provision directly points to two types of payment mandate. The first type is a payment mandate issued using a card, while the second one is a mandate issued with the use of an access code.

---

<sup>55</sup> Section 56 of the Payment Systems Act 2003 makes it an offence if the issuer failed to comply with the CC Guidelines.

Paragraph 15 extends the EFT Guidelines loss allocation scheme to a payment mandate issued with the use of an access code to cover the situation where the payment is made via distance payment facilities, such as telephone banking, where a specifically issued access code is used instead of a card.<sup>56</sup>

Apparently, Para 3's definition of an access code is, to "[include] [PINs], passwords, or code" [Emphasis added], which facilitates access to the consumer's account. The use of the word "include" indicates that an access code may consists of more than just the methods mentioned.<sup>57</sup> Hence, a literal approach to the rule would suggest that it might include the card details, which are used to issue a payment mandate on the internet and via the m-mobile payment systems.

However, the definition of an access code should be read in conjunction the rule in Para 15(1) (a) and (b), which imposes on the consumer a strict duty not to directly or indirectly disclose the "...code of his card" to anyone, and also to take a reasonable duty of care to protect the secrecy of the code. Since the person to whom the card is exposed can observe the details stated on the card, especially when the payment system is an offline system, the details cannot be an access code. It would be unfair to impose on the consumer a strict duty to protect the secrecy of the details, while the issuer is the one that should have developed a more secure system. Furthermore, Para 15(3), which

---

<sup>56</sup> Paragraph 4 of the EFT Guidelines defined electronic funds transfer to include transfer by means of telephonic instrument.

<sup>57</sup> The word "include" was defined in a *Rex v Latip Bin Haidin* [1935] 1 MLJ 84, at 86, to refer to non comprehensive or exhaustive definition of the term and in *Maplelee Property Sdn Bhd v Tan Lei Fon* [2005] 3 MLJ 305, at 361 the court held that "including" does not restrict or limit the scope of the contract term in which it used.

requires the consumer to inform the issuer of a breach of the access code security, indicates that an access code is something that involves a certain security protocol and cannot be the card details.

Another possible argument to bring the payment mandate issued using the card details under the EFT Guidelines, is to define the card details as a code to access the electronic device mentioned in the second proviso in Para 15(1)(a). This paragraph forbids the consumer to “directly or indirectly disclose to any person the access code to his card or any electronic device used to effect [an EFT]”.<sup>58</sup> Since an “electronic device” can be literally interpreted to refer to a contrivance,<sup>59</sup> albeit an electronic one, with a physical presence, like a computer,<sup>60</sup> or a mobile phone, where payment can be initiated using the card details, the access code should also include the card details. However, the language of Para 15(1) (a) cannot support this view. It should be noted that the conjunction “or” that joins the first and second part of the rule, is not followed by an “of”, which is used to indicate possession, before the phrase “any electronic device”.<sup>61</sup> Accordingly, it can be concluded that the “access code” only refers to the access code of the card but not of the electronic device.

From the above arguments, it is believed that the issuer does not have to apply the EFT Guidelines to assess the validity of the payment mandate issued using the card details.

---

<sup>58</sup> Paragraph 15 (1) “A customer shall not- (a) directly or indirectly disclose to any person the access code of his card or any electronic device used to effect an electronic funds transfer;”

<sup>59</sup> *Si Rusa Inn Sdn Bhd & Ors v Collector of Land Revenue, Port Dickson & Ors* [1987] 1 MLJ 147, at 152 per Peh Swee Chin J, and *Regina v. Munks* [1964] 1 Q.B. 304, at 306.

<sup>60</sup> *Wachter v. Denver Nat'l Bank*, 751 F. Supp. 906 (D. Colo. 1990).

<sup>61</sup> See the wording of the rule in n. 58 above.

However, the Guidelines are applicable when a disputed payment has been initiated using the card and/or the PIN or with the use of another access code issued to the consumer for electronic banking facilities.

It is clear that the losses caused by fraudulent credit card payment and EFT payment in Malaysia must be allocated by the issuer, according to CC Guidelines and the EFT Guidelines respectively. Nevertheless, the detailed rules in both set of Guidelines may give different levels of protection to the consumer. In particular, it was shown that the issuer might use its own loss allocation rules to determine the validity of the EFT payment mandate issued with the use of the card details. Similarly, the CC Guidelines can also be used to determine the validity of a payment mandate issued with the card but not the card details. In these circumstances, the issuer may provide in the contract the rules to be used to determine the validity of the payment mandate issued with the use of the card details. These rules may contain conditions of liability and methods of allocating the losses that are unfair to the consumer.

## **6      COMPARISON AND CONCLUSION**

The process of finding the party responsible for a particular payment begins with an assessment of the validity of the payment mandate that was acted upon by the issuer when it made a payment from the consumer's account. Accordingly, the loss allocation rules must govern not only the process of issuing the payment mandate but also the method of issuing the mandate.



The above discussion revealed the scope of the payment mandate under the credit card and the EFT loss allocation schemes used in the United States, the United Kingdom and in Malaysia. Basically, the loss allocation rules for the credit card and the EFT payment in all three jurisdictions discussed in this dissertation, linked the assessment of the payment mandate validity to the use of the cards and/or the access code. The limited scope of a payment mandate is evidenced by the reliance on terms such as “unauthorised use of a credit card”, “misuse of the credit token”, and “unauthorised transactions as a consequence of lost or stolen card”.

As a result of the references to the use of the card as a method of issuing the payment mandate, it appears that these loss allocation rules only facilitate the allocation of the losses if the fraudulent payment was made by the issuer who acted upon a mandate issued with the use of the card.

This implication creates uncertainty as to whether the losses that were caused by the fraudulent payment should be allocated according to the rules provided in the respective electronic payment systems’ regulations, if the mandate was issued using other materials such as the card details.

In the United States, the uncertainty can be avoided by a purposive interpretation of the TILA and the EFTA loss allocation rules. Moreover, the TILA and EFTA loss allocation schemes contain rules, in s. 133 (d) and s. 909(e) respectively, which made their scheme the ultimate scheme for allocating fraudulent payment in the two payment

systems. Therefore, read together, these two sections, with the purposive interpretation of the language of the TILA and the EFTA loss allocation rules, would help to protect the consumer in circumstances where the payment was initiated with the use of the card details.

On the other hand, in the United Kingdom, a specific regulation was passed to protect the consumer against losses caused by unauthorised payment in a distance transaction. Regulation 21 of the DSRs, which is now incorporated in s. 84(3A) of the CCA and s. 12.12 of the Banking Code, provides that the losses caused by a fraudulent payment in a distance transaction are to be allocated to the issuer. This rule is very wide to cover an unlimited scope of a payment mandate, including the mandate issued with the use of the card details.

Unfortunately, in Malaysia, the CC and EFT Guidelines do not have any rule identical to Reg 21 of the DSRs, which remedies the uncertainty in relation to the validity of a payment mandate issued using the card details. Perhaps, the only possible remedy under the CC Guidelines is to interpret the rule in Para 13.2 in a wider sense to cover the mandate issued with the card details.

Accordingly, it can be concluded that, in so far as the protection of the Malaysian consumer is concerned, unless and until the internet or the m-payment systems accept the card, or a system is developed to facilitate secure process of giving instruction with the card details, a consumer who used the internet or the m-payment systems may be

exposed to a bigger amount of losses than those who used the card to initiate the payment. Moreover, even if the PIN is used, (it is usually given after the consumer had successfully registered) still at the initial registration stage, the consumer has to type the card details into the internet or the m-mobile payment systems. Accordingly, if others intercepted the communication and used the details obtained by illegal access to issue a payment mandate, the issuer may assess the validity of that mandate, based on its own rules, which may prejudice the protection of the consumer against fraudulent payment.

Another important conclusion to be deduced from the above discussion is that the assessment of the validity of the payment mandate is most of the time linked to a single access mode and not to a combined mode of access. For instance, in the case of the credit card, it was always referring to the card and not to the card and the PIN, which is a combination now used in almost every corner of the world to initiate credit card payment at the POS terminal. The reference to an individual and independent mode of issuing a payment mandate in the loss allocation rules also creates ambiguity as to whether the validity of a payment mandate issued using a combined method is to be assessed based on the respective loss allocation rules.

In the United States, the decision in *Ognibene v Citibank, N.A.*<sup>62</sup> which involved the EFTA loss allocation rules showed that a payment mandate issued with the use of the card and the PIN where the card was obtained with consent while the PIN was obtained by an illegal means, is a fraudulent payment mandate. This decision showed that under

---

<sup>62</sup> 112 Misc.2d 219, 446 N.Y.S.2d 845, 847, (1981).

the EFTA, the validity of the payment mandate issued with a combined access mode must also be assessed according to the EFTA loss allocation rules.

Similarly, in the United Kingdom, the Banking Code rules can also be interpreted to apply to a payment mandate issued using a combination of a card and a PIN. The same comment would also apply to the Malaysian EFT Guidelines which show that the access code and the card are vulnerable to unauthorised use. Hence, a combination of the two may be used to issue a payment mandate, the validity of which must be assessed according to the EFT Guidelines loss allocation rules.

Finally, in the United States, there is uncertainty as to the applicability of the TILA loss allocation rules to assess the validity of a mandate issued with the use of a combination of a credit card and a PIN. However, it should be noted that s.133 (a) (1) (F) of the TILA requires a suitable identification method to be given to the consumer before any unauthorised payment loss can be allocated to him. Since the PIN is usually used to identify the card user, it is safe to conclude that the validity of a mandate issued in a system which requires the use of a credit card and a PIN must also be assessed according to the TILA loss allocation rules.

# **CHAPTER THREE            THE MANDATE RULE AND THE LOSS ALLOCATION RULES IN THE CREDIT CARD AND EFT PAYMENT**

## **1 INTRODUCTION**

In the discussion in Chapter two it was shown that the loss allocation schemes in the three jurisdictions apply to certain types of access modes only. As a result, the loss allocation rules can be applied to access the validity of the payment mandate issued with the use of these respective modes only except when the rules are liberally interpreted using the purposive rule.

This chapter will further analyse these loss allocation rules to examine the circumstances and conditions when the credit card or the EFT payment initiated with the use of the access method is considered as valid and binding on the consumer.

There are four parts to the discussion. Part two to four discuss the loss allocation rules that are applicable in the credit card and EFT payment systems in the United States, the United Kingdom and Malaysia respectively. Part five concludes the discussion by highlighting the various rules, and the strength and weaknesses of the rules in protecting the consumer against the losses caused by fraudulent payment.

## **2 THE MANDATE RULES IN THE UNITED STATES**

The TILA and the EFTA together with their respective regulations, Reg. Z and Reg. E, incorporate the agency rule of actual, and apparent authority to determine the validity of the payment made from the consumer's account. The following discussions highlight the essential features of these rules and their effect on the allocation of fraudulent payment losses.

### **A Unauthorised Credit Card and EFT Payment and the Actual Authority**

In Chapter two, it was shown that unauthorised payment occurs in many circumstances including when the credit or debit card is lost or stolen.<sup>1</sup> It was also shown that in certain circumstances, the payment initiated with the use of the card details or the access code could also become an unauthorised payment.<sup>2</sup> The general rule is that when and if the person who initiated the payment did not have the authority to make the respective transaction, the payment was unauthorised and did not bind the consumer.

Consequently, a consumer is responsible for the respective credit card or EFT payment when the person who initiated the payment possessed the actual authority to make the transaction. Actual authority means an express or implied authority that is granted by

---

<sup>1</sup> See Chapter two at 44-45, 54, 60-61.

<sup>2</sup> Ibid, at 49-50, 51-53 56-57 59, and 61.

the consumer to another person through his words and/or actions authorising that person to make a payment from his credit card or EFT account.<sup>3</sup>

The agency rule of actual authority is incorporated in s.103 (o) of the TILA and in footnote 22 to s. 226.12(b)(1) of Reg. Z. Both provisions describe authorised credit card payment as a payment made by the issuer upon receiving a mandate issued by a person who possesses either an express, implied or an apparent authority.<sup>4</sup>

A slightly different description is given to an authorised EFT payment. Section 903 (11) (A) of the EFTA and s.205. (m) (1) of Reg. E. described authorised EFT payment as a payment initiated by a person who possesses actual authority. The description seems to suggest that an EFT payment initiated by a person who has an apparent authority is not a valid payment. However, further reading of the EFTA shows that s. 903(11)(A) binds the consumer to the payment made by a person who was once authorised by the consumer to use the access device even after that person's authority was terminated if the termination notice was ineffective.<sup>5</sup> The requirement of notification to terminate the authority of a person to initiate the EFT payment shows that the EFTA loss allocation rules also allocate losses based on an agency rule of apparent authority.

---

<sup>3</sup> See s. 7 and s. 23 of the Restatement (Second) of Agency 1958.

<sup>4</sup> To determine the presence of any type of the authorities mentioned, reference is to be made to the relevant state law that governs the contract between the consumer and the issuer. The states law however mostly follow the Restatement (Second) of Agency. See s. 8, s. 26 and s.27.

<sup>5</sup> See also s. 205.2 (m) (1) of Reg. E.

However, it should be noted that the TILA and the EFTA do not describe in clear terms the circumstances when a person becomes an authorised person. As such, it is necessary to refer to judicial decisions which interpret the rules in order to identify the circumstances that create the authority and also the type of authority possessed by the person who initiated the payment.

*(a) Transfer of the consumer's card and/or the PIN to the user*

The most straightforward way to give someone with the actual authority to initiate a credit card payment is by transferring the credit card to him or her and expressly telling him or her to use the card. This act was a cause for dispute in *Martin v. American Express, Inc*<sup>6</sup>. Mr Martin gave his credit card to his business partner to be used for the purpose of their business, telling his partner to use it to a maximum of \$500. The card was used beyond the \$500 limit and Mr Martin refused to pay. The issuer's claim for repayment was granted by the court. It was held that s.133 (a) of the TILA which protects the consumer against unauthorised credit card usage, is not applicable if the consumer voluntarily and knowingly allows another person to use his card and that person subsequently misused the card.

The same consequence follows if the consumer gave his debit card or other mode of access to his account to the one who initiated the EFT transaction. The applicability of the agency principle to the EFTA loss allocation rules was established in the case of

---

<sup>6</sup> 361 So.2d 597,599 Ala. Civ. App. 1978.



*Ognibene v Citibank, N.A.*<sup>7</sup>. It is interesting to see that in this case, Mr Ognibene gave his ATM card to the fraudster. Under the agency rule, that act would amount to actually authorising the recipient to initiate the fund transfer.<sup>8</sup> However, it was proven that the consumer must use the PIN and the card in order to access his account via the ATM machine. Considering the essential function of the PIN, the court decided that the consumer's voluntary transfer of the card did not clothe the card user with an actual authority to initiate the transaction when the PIN was obtained by the user through an illegal action.<sup>9</sup>

The court in *Ognibene's* case did not constrain itself by the form of the access device which passed from the consumer to the fraudster. Instead it took a functional approach and decided that when the account requires a combined access method but only part of the method is obtained with the consumer's consent while the other part was wrongfully obtained the person who initiated the EFT transaction did not have the actual authority to make the transaction.

The approach taken by the court was in conformity with the definition of the "access device" in s. 205.2 (a)(1) of Reg. E which includes "any combination" of the card and/or PIN or other means of accessing the consumer's account. In fact, the decision in *Ognibene's* case can also be supported by reading together s. 205.2 of the Reg. E and its

---

<sup>7</sup> 112 Misc.2d 219, 446 N.Y.S.2d 845, (1981) at 847.

<sup>8</sup> Melley, A. E., "Generally; express authority", and "Implied and Incidental Authority- Extent", 3 *Am.Jur.* 2d Agency, s 70 and s. 72.

<sup>9</sup> See s. 205.2 (m)(1) of Reg. E which provides that unauthorised transfer occurred if a person instructing the transfer was given the access device by the accountholder. See also the staff interpretation in s.205.2 2(a).

respective Staff Interpretation, which shows that an access device refers to the “means that may be used by a consumer to initiate an [EFT] to or from a consumer account”.<sup>10</sup> Since the access to Ognibene’s account via the ATM machine required the card and the PIN, where the card was worthless without the PIN, it means that the card alone did not constitute an access method. Accordingly, the court was correct when it held that the transfer was not initiated by a person who possessed actual authority to access the account.

Compared to the EFTA, the definition of an unauthorised payment in the TILA specifically refers to unauthorised use of a credit card.<sup>11</sup> This definition clearly indicates that the only means of accessing the account is via a credit card. Therefore, it is assumed that the actual authority can be granted only by giving the card to the user without other material even if the particular transaction would require the use of a credit card and its associated PIN.

If the above were a correct position, a consumer in a situation like Mr Ognibene would be liable for unauthorised credit card transactions because he had given the credit card to the user, thereby authorising him to use the card. This limited definition of an unauthorised credit card payment is not in keeping with the current practice of using a combination of a card and PIN.

---

<sup>10</sup>Section 205.2 (2) (a) of the Official Staff Interpretation to Reg. E.

<sup>11</sup> See Chapter Two at 45-48 and 50-58.

However, as argued earlier, the constructive interpretation of the rule in s. 133 of the TILA suggests that the mode of issuing the mandate may include the use of the credit card details.<sup>12</sup> Therefore, when this type of construction of the TILA rules extends the TILA protection to cases where the payment does not involve the card, it is believed that the protection can also be extended to cover the cases where the payment requires the card and the PIN. In fact, the use of a credit card and the associated PIN to initiate the credit card payment is even closer to the scope of unauthorised credit card payment which involved “unauthorized use” of a credit card.

Therefore, in a transaction where both the card and PIN or the card details are needed to initiate a credit card payment, a wider interpretation of the rule in s. 133 would consider the act of giving the card or the card details, or the card and the PIN to the user as giving an actual authority to him to initiate the payment.

*(b) Additional card holder and actual authority*

In both the TILA and the EFTA loss allocation rules, a person may also possess an actual authority when he is appointed as an additional card holder. Hence, when the wives in the *Walker Bank & Trust Co. v. Jones*<sup>13</sup> appointed their husbands as additional card holders, the court found the wives responsible for the charges made by the husbands who used the credit cards issued to them by the issuer.

---

<sup>12</sup> Chapter Two, at 49-50.

<sup>13</sup> 627 P.2d 73, 77 Utah 1983.

The court would reach the same decision if the dispute involved an EFT payment. Accordingly, any payment initiated with the use of the debit card issued to an additional card holder binds the consumer.<sup>14</sup> This authority continues to exist until the consumer successfully terminates it.<sup>15</sup> However, the notice of termination of the authority will only protect the consumer against the losses from subsequent fraudulent payment but not for past payments. This rule is to be understood from the purpose of the notification which is to enable the issuer to take action to prevent further unauthorised payment. This matter is discussed below in a discussion involving the application of an apparent agent's authority in the allocation of fraudulent payment losses.

## **B      Unauthorised Credit Card and EFT Payment and the Apparent Authority**

Apparent authority requires a total examination of the circumstances that create a belief in the mind of the issuer that the person issuing the mandate was authorised to act on behalf of the consumer.<sup>16</sup> For instance, a consumer may have terminated the authority of an additional card holder to use the card but failed to retrieve the card. The consumer's failure to prevent continuous possession of the card represents to other persons that the card holder is an authorised person.<sup>17</sup>

---

<sup>14</sup> *Kruser v. Bank of America* 230 Cal.App.3d 741, 281 Cal.Rptr. 463 Cal.App. 5 Dist.,1991.

<sup>15</sup> Section 125 and s. 136 of the Restatement (Second) of Agency 1958. R. A. Lord (Ed), *Williston: A Treatise on Contracts*, 4<sup>th</sup> Edn, (1990-2004) s. 35:30, West Group. (Hereafter *Williston: A Treatise on Contracts*).

<sup>16</sup> *Williston: A Treatise on Contracts*, §35:14-17.

<sup>17</sup> *Ibid*, §35:17. See *Walker Bank & Trust Co. v Jones* 672 P.2d 73, 1983.

Similarly, apparent authority is also created if the user's authority is limited to a certain type of transaction or a certain amount of purchases while the other contracting party did not know about the limitation.<sup>18</sup> Apparent authority also exists if the card bears some information which indicates the type of transaction it was designated for, and it was used to pay for the transaction that falls within that designation even if the user went beyond the authorised limit.<sup>19</sup>

Apart from that, continuous payment of the unauthorised charges while knowing that they were unauthorised also creates an apparent authority. Consequently the consumer is barred from claiming the capped liability in s. 133 of the TILA.<sup>20</sup> Moreover, an apparent authority is also created if the consumer misrepresented to the issuer that the card, which was used to make the purchase, was in his possession, while in reality, it was taken away by the holder.<sup>21</sup> Finally, failure of the consumer to notify the issuer of the loss or theft of the card also creates an apparent authority in the person who used the card.<sup>22</sup>

With regard to the EFTA, though the definition of unauthorised funds transfer in s. 903 (11) did not specifically refer to an apparent authority, yet the notification rule in s. 909 (a) (2) suggests that apparent authority is also part of the EFTA loss allocation rules.

---

<sup>18</sup> See *Cities Service Co. v Paillet* 452 So.2d 319 La.App. 4 Cir., 1984 and *Martin v American Express, Inc.* 361 So.2d 597 Ala.Civ.App., 1978.

<sup>19</sup> *Towers World Airways v. PHH Aviation* 933 F.2d 174 (2d Cir.), cert. denied, 112 S.Ct. 87 (1991).

<sup>20</sup> *DBI Architects, P.C. v. American Express Travel-Related Services* 388 F.3d 886 C.A.D.C., 2004, at 370.

<sup>21</sup> *Oclander v. First Nat'l Bank of Louisville*, 700 S.W.2d 804 (Ky.Ct.App.1985).

<sup>22</sup> Section 133 (A) (1)(E) of the TILA, s. 226.12 (b) (1) (3) Reg. Z and s. 909 (a) (2) of the EFTA and s. 205.6 (b) Reg. E.

However, the reliance on the apparent authority as a basis for allocating the fraudulent payment losses sometimes creates a problem for the consumer if the access method was used after the user's authority had been terminated or when the consumer set a limit on the authority but the person went beyond that limit. The following discussion examines the protection given by the TILA and the EFTA to the consumer against unauthorised payment in these circumstances.

(a) *Apparent authority, notice to terminate the authority and the return of an access device*

Previously, it was presented that a consumer may appoint another person as an additional card holder and by doing that, he gives that person the actual authority to initiate a payment using the access device. However, by appointing the additional card holder, the consumer runs the risk of being liable for the losses caused by any unauthorised use of the mode of access by that person after his authority is terminated or when the transaction exceeds the limit of the actual authority.

In order to protect the consumer from the losses caused by unauthorised payment in those circumstances, it was necessary that the TILA and the EFTA specified the methods to be used by the consumer to terminate the authority and also the effect of the notification.

The TILA loss allocation rule in s.133 (a) (1) (E) provides that the consumer may limit his liability for unauthorised credit card use by giving to the issuer notice of the termination of the user's apparent authority.<sup>23</sup> This rule corresponds to the agency rule in s.136 of the Restatement (Second) of Agency (1958) which provides that notice given to a third party of the limitation set on an agent's authority will limit the agent's apparent authority to act on the principal's behalf.

It should be noted that the rule in s. 133 (a) (1) (E) of the TILA refers only to a notification of loss, theft or other form of involuntary transfer of the credit card.<sup>24</sup> It does not refer to a case where a person whose authority was terminated or limited misused the card that was initially given to him voluntarily. Accordingly, it is necessary to analyse judicial interpretations of the TILA rules in order to determine the consumer liability in case of misuse.

A significant case in relation to this issue is *Walker Bank & Trust Co. v. Jones*.<sup>25</sup> The defendants entered into credit card facility contracts with the issuer. They also agreed to appoint their husbands as additional card holders. The credit agreements required the wives to return all the credit cards if they wished to terminate the credit agreements. However, when the husbands absconded with their additional cards, the wives gave notice to the issuer to terminate the husbands' authorities. However, they did not give

---

<sup>23</sup> See agency rule on termination of agent's authority in s. 125 comment b and s. 136 of the Restatement (Second) of Agency 1958.

<sup>24</sup> See chapter two at 43-45.

<sup>25</sup> 672 P.2d 73 (Utah 1983), cert. denied, 466 U.S. 937 (1984).

notice to terminate the credit agreements. They also failed to return the husbands' credit cards. The husbands continued to use the cards. The wives refused to pay the charges, claiming that they had terminated the husbands' authority by giving notice of their intention to the issuer.

It was decided by the majority that, regardless of the notification, the consumers' failure to return the card, which allowed the husbands to have continuous possession, enabling them to use the cards, manifested to the merchants that the husbands possessed the authority to use the cards to initiate the disputed payments. Moreover, it was also held that the notices given by the consumers could not terminate the apparent authorities of the husbands because the TILA requirement of notification as a mode of terminating the agent's authority, applies only to the case of an involuntarily transfer of the card but not to cases of misuse of the card by an authorised holder.<sup>26</sup>

Regardless of the majority, the dissenting judge was of the view that the notification rule in s. 133 of the TILA should be interpreted by taking into account the purpose of the TILA, which includes the protection of the consumer against fraud losses; hence preferring the issuer's liability for the losses.<sup>27</sup> Accordingly, the notice given by the consumers should have been effective in terminating the husbands' authority even if the consumers had failed to retrieve the cards and return them to the issuer. Moreover, it

---

<sup>26</sup> See comment on this issue in Mathews, M. E., "Credit Cards--Authorized and Unauthorized Use" (1994) 13 *Ann. Rev. Banking L.* 233, at 287-292. (Hereafter Mathews, M. E., Credit Cards--Authorized and Unauthorized Use). See also *Oclander v. First National Bank of Louisville* 700 S.W.2d 804 (Ky. App. 1985) and *Martin v. American Express, Inc* 361 So. 2d 597 (Ala. Civ. App. 1978).

<sup>27</sup> 672 P.2d 73 Utah, 1983, at 76-79 *per* Durham, J, with Howe J concurring.



was also revealed that the credit agreements contained clauses which required the consumers to inform the issuer of potential unauthorised credit card use in order to limit their liabilities.<sup>28</sup> Referring to this clause, the dissenting judge was also of the view that the consumers' failure to terminate the credit agreements did not affect their liabilities because the notices which they sent to the issuer telling it of the potential unauthorised payment was sufficient to terminate the husbands' apparent authority.

A similar decision was reached in *American Exp. Travel Related Services Co., Inc. v. Web, Inc.*<sup>29</sup> The case was about misused of credit card by an additional card holder. In an appeal by the account holder against the Court of Appeal's decision that the payments were authorised, the Supreme Court emphasised that: "[in] setting out the limits of the liability of credit consumer in [section 133 of the TILA] Congress did not provide for mitigation of card holders' liability by notification of misuse to the issuer."<sup>30</sup> It also emphasised that notice of misuse does not convert the card holder into an "unauthorized" user.

A contrasting view as to the effect of the notice in s. 133(a) (1) (E) of the TILA appears in *Standard Oil Company v. Steele's*.<sup>31</sup> In this case, the user obtained the consumer's consent to charge the consumer's card for the purchase of a tank of fuel. After the return of the card, further purchases were charged to the consumer's credit card account. The

---

<sup>28</sup> Ibid, at 79.

<sup>29</sup> 261 Ga. 480, 405 S.E.2d 652 Ga.,1991.

<sup>30</sup> Ibid, at 482.

<sup>31</sup> 489 N.E.2d 842 (Ohio Mun. 1985). See similar decision in *Cities Service Co. v. Paillet* 452 So.2d 319 La.App. 4 Cir.,1984.

consumer notified the issuer of the misuse of the card and disputed the charges under s. 133 of the TILA. The court held that the payments made after the notification were unauthorised.

The court in this case interpreted the word “unauthorized” use in the notification rule in s.133 (a)(1)(E) of the TILA to include the credit card transaction made by a person after his actual authority was terminated by the card holder.

Although the above decisions show that the consumer cannot limit his liability for credit card misuse, there are circumstances where card usage by a person whose authority was terminated falls within the scope of unauthorised use under s. 103 of the TILA. For example in *Blaisdell Lumber Co., Inc. v. Horton*<sup>32</sup>, and *Vaughn v. United States Nat'l Bank of Oregon*,<sup>33</sup> it was found that payments made by persons whose authority to use the consumers' credit cards were terminated were unauthorised because the users took the cards by way of stealing. In these cases, the consumers successfully proved that when the users took the cards for the second time and initiated the disputed payments, it was done without the consumers' consent. Accordingly, when the consumers informed the issuers of the potential unauthorised payment, the notices were sufficient to protect them from the payments made after the notification.

---

<sup>32</sup> 242 N.J.Super. 98, 575 A.2d 1386 (App.Div.1990).

<sup>33</sup> 79 Or.App. 172, 718 P.2d 769 (1986).

The decisions in these two cases supported the finding in *Walker* and other cases where unauthorised credit card usage was held not to include credit card misuse even if the use took place after the consumer terminated the user's actual authority. Moreover, the decisions showed that for the termination of the user's apparent authority to be effective, the consumer must take possession of the card.

Apart from those cases, there are two other cases which support a different finding. The first one is a Californian case of *Young v. Bank of America Nat'l Trust & Sav. Ass'n*.<sup>34</sup> The consumer disputed the credit card charges made to her account by her friend to whom the consumer had given the card for a specific limited transaction. The issuer refused to treat the charges made after the consumer's notification of loss of the card as unauthorised. The issuer firmly emphasised that the card was voluntarily given to the user. However, the court referred to the Californian Civil Code section 1747.02, subdivision (f) which has provisions which closely resembled the rule in s. 103 of the TILA, and decided that the notice effectively terminated the card user's authority and eventually limited the consumer's responsibility for the charges made with his consent.

Although this decision contradicts the majority of other cases, it also found support in the Federal Trade Commission Consent Order against the *Shell Oil Co.*<sup>35</sup> In this Order, the FTC required the issuer to stop its violation of the rule in the Reg. Z by ending its

---

<sup>34</sup> 141 Cal. App. 3d 108, 190 Cal. Rptr. 122 (1st Dist. 1983).

<sup>35</sup> 1980 WL 338998, 95 F.T.C. 357 (1980).

practice of allocating the liability for credit card misuse to the card holder who had terminated the user's authority by notification.

These two last cases are the best from the consumer protection perspective because they conform with the purpose of the TILA, which is to protect the consumer against fraudulent payment. In particular, in both cases, the court and also the commission interpreted the notification rule in s. 133(a) (1) (E) of the TILA to apply to cases of unauthorised use of the credit card and also the case of misuse of the card.

The above interpretation of the TILA's notification rule is best from the consumer protection perspective since it is hard for the consumer to gain control of a card which was taken away by the holder. In some cases, it is as hard as getting it from a thief. Moreover, the facts in *Oclander v First Nat'l Bank of Louisville's* case,<sup>36</sup> where the issuer blocked the use of an additional card issued to a man, after receiving notice from his wife of their separation, showed that it is not uncommon for the card issuer to block a credit card account from the additional card charges when the card was taken away by its holder. So the same practice can be used by the issuer to stop credit card misuse upon receipt of a notice of potential misuse by the consumer

The above problem is however, not an issue in the debit card payment system. Even if the consumer has given his own debit card to another person or appointed another as an additional card holder, s.903 (11)(A) allows the consumer to terminate the user's

---

<sup>36</sup> 700 S.W.2d 804 (Ky.Ct.App.1985)

authority by simply giving notice of that intention to the issuer. In other words, under the EFTA, the issuer cannot require the consumer to return the debit card as a condition for an effective termination of the card holder's authority because it would be contrary to the EFTA rules and invalid by virtue of s. 909 (1)(e).

(b) *Apparent authority and the person to be served with the notice of termination of authority*

Agency law requires the principal to inform the person with whom the agent had dealt with on his behalf, and the person he is likely to know of his intention to terminate the agent's authority.<sup>37</sup> In particular, s. 136 (2) (d) of the Restatement Second of Agency states that if the agent possesses an item which represents his authority to act on behalf of the principal, the latter must give notice to terminate that appearance of authority to the person to whom the item is shown. Therefore, when the consumer gave a credit card to the user, he can only terminate that authority by giving notice to that effect to the third party who relies on the card usage as an indication of the card user's authority.

Although the rule seems to be very clear, yet its application under the TILA is less than straightforward because the TILA does not specify the party to be served with the notice. In fact, the uncertainty is found in several judicial decisions which pointed to differences of opinions among the judges with regard to this issue.

---

<sup>37</sup> Melley, A. E. "Notice to third persons", 3 *Am. Jur.* 2d, Agency, s. 50.

In the case of *Towers World Airways v. PHH Aviation*<sup>38</sup> for instance, the Appeal Court, while referring to the decision in *Walker*<sup>39</sup> and other cases, decided that a notice to the issuer to limit the agent's authority would only cap the consumer's liability in the case of a three-party arrangement (tripartite), where the issuer and the merchant acquirer are the same party but not in a four-party arrangement, where the merchant acquirer and the issuer are different entities.<sup>40</sup>

The court reached the conclusion by emphasising that agency law requires the notice to be given to a third party who acted as a result of his reliance on the appearance of the authority of the purported agent. Since in the tripartite arrangement the merchant and the issuer are the same person, the notice given to the merchant is effective to limit the card holder's liability for the unauthorised payments.<sup>41</sup>

The court in the *Walker Bank & Trust Co. v. Jones*<sup>42</sup> also explained that the merchant was the third party to be informed of the potential unauthorised payment if the notice referred to in s.133 of the TILA was to be effective in terminating the user's apparent authority in a case of credit card misuse. Apparently, in *Tower*, the custom of the aviation industry where the pilot is given the card to make "air-plane cases related purchase" and in *Walker* the husbands' names on the cards, manifested to the merchant

---

<sup>38</sup> 933 F.2d 174 (2d Cir.), cert. denied, 112 S. Ct. 87 (1991).

<sup>39</sup> *Walker Bank & Trust Co. v. Jones* 672 P.2d 73 Utah, 1983.

<sup>40</sup> The court argument was "In four-party arrangements of this sort, it is totally unrealistic to burden the card issuer with the obligation to convey to numerous merchants whatever limitations the cardholder has placed on the card user's authority".

<sup>41</sup> *Supra* 38, at 178-179.

<sup>42</sup> 672 P.2d 73 Utah, 1983, at 76.

of the card users' apparent authority. Accordingly, the notice has to be given to the merchant. This finding is in line with the rule in s. 136 (2) (d) of the Restatement Second of Agency.

A similar decision was reached in *American Exp. Travel Related Services Co., Inc. v. Web, Inc.*<sup>43</sup> where the credit card was misused by an additional card holder. When the account holder appealed against the Court of Appeal's decision that the payments were authorised payments, the Supreme Court emphasised that: "[in] setting out the limits of the liability of credit consumer in [section 133 of the TILA] Congress did not provide for mitigation of card holders' liability by notification of misuse to the issuer".<sup>44</sup>

On the other hand, in *Transamerica Insurance Co. v. Standard Oil Co.*,<sup>45</sup> the court held that the issuer was the third person to whom the appearance of authority was created. Although the issuer was at the same time the merchant, the card could also be used to purchase goods and services with other merchants. The court decided that notice was to be given to the issuer who was also a merchant. From the decision it appears that the court treated the issuer as the third party, in the capacity as an issuer and not as a merchant. This is to be understood from the court's decision where it concluded that apparent authority was created by the account holder's failure to examine the statement of account and its continuous repayments of the charges made by the user. Since the account holder failed to examine the account statement, and consequently failed to

---

<sup>43</sup> 201 Ga.App. 202, 410 S.E.2d 830 Ga.App. 1991.

<sup>44</sup> 261 Ga. 480, 483, 405 S.E.2d 652 Ga., 1991.

<sup>45</sup> 325 N.W.2d 210 N.D., 1982, 216.

notify the unauthorised charges and also continued making repayments, which were acts committed in relation to the issuer in its capacity as an issuer and not as a merchant, the notice to terminate the authority ought to have been given to the issuer not the merchant.

Based on those decisions, it is clear that the notification rule in s. 133 (a) (1) (E) of the TILA created uncertainty as the person to whom the notice of potential unauthorised payment should be given by the consumer. If the rule is interpreted to require the consumer to examine whether the credit arrangement is a tripartite or four-party arrangement before he gives notice of an unauthorised payment, the rule imposes on the consumer extra responsibility to examine and learn about the credit arrangement before he can make an effective notification. This interpretation will also affect the protection of the consumer against unauthorised payment since some consumers may not understand the credit card arrangement. By adopting this interpretation it also means that the rule failed to recognise the issuer's financial and technical ability to communicate to the merchant a warning against accepting the credit card the credit card network facility such as the regional credit card bulletin.<sup>46</sup>

The EFTA rule on notice of termination of apparent authority differs from the TILA's rule. Section 903(11)(A), specifically required the notice to terminate the user's apparent authority to be given, to the issuer. By fixing the issuer as the one to whom the notice is to be given this section prevents the difficulty of finding the third party in a

---

<sup>46</sup> Weistart, J. C, *Consumer Protection in the Credit Card Industry: Federal Legislative Controls* (1972) 70 *Michigan Law Review*, 1475, at 1509-1510. (Hereafter Weistart, J. C, *Consumer Protection in the Credit Card Industry: Federal Legislative Controls*).



transaction which involves more than two parties as discussed earlier. This rule successfully eliminated the need to rely on the agency principle to determine the person to whom the termination of the apparent authority is to be notified.<sup>47</sup>

*(c) Apparent authority and the duty to examine the statement of account*

Before the TILA was passed, the consumer's failure to examine the statement of account may have prevented him from denying the validity of the payment made using his access device though silence by itself does not constitute *estoppel*.<sup>48</sup> The consumer is estopped from denying the validity of the payment because his failure to notify the issuer of the unauthorised payment that he discovered in his account statement amounted to a misrepresentation that the person who initiated the payment was an authorised person.<sup>49</sup>

There are several cases in which the court applied the *estoppel* principle in disputes involving credit card transaction. For example, in *Sinclair Refining Co. v Consolidated Van & Storage Cos.*<sup>50</sup> the credit cards' account holder had allegedly sold his business to a third party and allowed the truck drivers of the third party to use the credit cards. The account holder did not notify the issuing company of this change, despite continuing to

---

<sup>47</sup> See Matthews, M. E., "Credit Cards--Authorized And Unauthorized Use, .for a discussion on finding the third party in the case of a credit card payment.

<sup>48</sup> Williston, *A Treatise on Contracts*, §§ 8.3-8.6. See also Comment c to s. 8B of the Restatement (Second) of Agency 1958 and the case of *DBI Architects, P.C. v. American Express Travel-Related Services* 388 F.3d 886, C.A.D.C, 2004 at 891.

<sup>49</sup> Comment d to s. 8B of the Restatement (Second) of Agency 1958 provides, "When one realizes that another is or may come under a misapprehension as to the authority of his agent or the ownership of his property, a misapprehension for which he is not at fault, his duty to give information is a duty of due care."

<sup>50</sup> 192F Supp. 87 DC Ga, 1960.

receive monthly statements which recorded purchases made to the account. The court on granting summary judgement held that the account holder was *estopped* from denying the recovery of the payment by the issuer since he had acquiesced in the purchases.

Similarly, in *Neiman-Marcus Co. v Viser*<sup>51</sup>, a husband who gave his store-card to his wife before they separated was held liable for purchases made by the wife using the card after their separation. The court found the presence of an apparent authority which prevented the consumer from claiming the lack of authority of the wife.

Apparently, in pre-TILA's cases, the equitable principle of *estoppel*<sup>52</sup> was applied to determine the account holder's liability for a credit card payment made by a person who did not possess an actual authority to initiate the payment. The equitable estoppel referred to in the *Neimans* and *Sinclair* cases operates on a principle identical to that of apparent authority, that is, to serve justice so that as between two innocent parties "[the person] who has enabled such third person to occasion the loss must sustain it."<sup>53</sup>

However, it is essential to see whether the same *estoppel* is applicable to the loss allocation rules under the TILA. In other words, will the consumer's failure to examine

---

<sup>51</sup> 140 So 2d 762. La. App. 1962.

<sup>52</sup> Section 8B of Restatement Second of Agency. See also 31 C.J.S. Estoppel and Waiver § 58, Estoppel and Waiver, and Reynolds, F. M. B., Bowstead and Reynolds on Agency 18th Edn (2006), § 8.09, Sweet & Maxwell. (Hereafter Reynolds, F. M. B., Bowstead and Reynolds on Agency).

<sup>53</sup> *Hunsakar v Rhodehouse* 77 Idaho 119, 289 P.2d 319 (1955).

his statement of account prevents him from denying his liability for the disputed credit card payment.

The first case which can highlight the issue is *Minskoff v. American Exp. Travel Related*.<sup>54</sup> In this case, the account holder disputed the charges made to his credit card account by an employee who forged the account holder's signature and applied for two supplementary credit cards for her personal use without his knowledge. All the charges made with the supplementary cards were recorded in the statements of the accounts sent to the account holder's business address. Being a personal assistant to the account holder, the employee took care of the statements and paid the charges including the charges made by her with the company's cheques. The court found the account holder liable for the charges since his failure to examine the statement of account amounted to a negligent manifestation of the card user's authority to initiate the credit card payments.

In its decision, the court interpreted the loss allocation rule in s. 133 of the TILA by importing the negligence rule which is a trait of the law of banking. The court commented that the account holder had acted negligently by failing to examine the statement of account which would have revealed the unauthorised payments. In fact, he should be responsible for the losses because his negligence had created the appearance of authority in the employee to use the cards.<sup>55</sup>

---

<sup>54</sup> 98 F.3d 703 C.A.2 (N.Y.),1996, at 709.

<sup>55</sup> Ibid, at 170.

However, there are two new cases that contradict the above decision. The first case is *DBI Architects, P.C. v. American Express Travel-Related Services*.<sup>56</sup> The facts of this case are identical to the *Minskoff* case. One of the company's employees applied for a corporate credit card without the company's authority. The statements were sent to the company's business address and the employee forged the company's cheques in order to pay for the charges. The company disputed the charges and refused to pay the balance on the statements, claiming that the payments were unauthorised.

Applying the agency rule of apparent authority, the court held that the account holder's failure to examine the statement of account did not amount to a manifestation of card user's authority. Rather, apparent authority was created by the account holder's repeated payments for the credit card usages, after receiving the statement which contained the unauthorised charges. The court emphasised that a mere silence did not create an apparent authority.

The DBI's decision was followed by the case of *Carrier v. Citibank (South Dakota)*.<sup>57</sup> In this case the employee worked with the Carrier family's business. She used the credit card number of one of the Carrier family members to make some purchases. She also took the credit card issued to that person and charged it for certain purchases. When the statement arrived at the business address, the employee used the company's cheques signed by the Carrier to pay for the charges.

---

<sup>56</sup> 388 F.3d 886 C.A.D.C.,2004.

<sup>57</sup> N.A. F.Supp.2d, 2005 WL 2002484 D.Conn.,2005.

Again in this case, the court attached the account holder's liability to a series of payments made by the Carrier to the issuer, using the business cheques which bore their signatures.<sup>58</sup> According to the court, the consumer's act of continuing to pay for the charges with the company's cheques created a belief that the person who initiated the payment was authorised to do so.

The decisions in the above cases have two implications. First, the consumer did not give a credit card user apparent authority, merely by failing to examine his account statements. Second, the decisions showed that it is possible to find the presence of an apparent authority when the consumer's failure to examine his statement of account prevents him from detecting unauthorised payment and consequently, continues to repay the issuer for the charges made to his account. Accordingly, it can be concluded that the decisions in the *DBI's* case and also the *Carrier's* case, though short of imposing a duty, indirectly required the consumer to examine the statement of accounts, because if he failed to do that, he would be paying the fraudulent charges, which may form a manifestation of the card user's authority.

It should be noted that, the EFTA loss allocation rules are better drafted to handle the issue of apparent authority created by a consumer's failure to report any unauthorised payment which is recorded in the account statement. Section 909(a) provides that a consumer has to examine his account statement and to report to the issuer any unauthorised transaction found in the statement. This rule removes the problem faced

---

<sup>58</sup> Ibid, at 6.

by the consumer under the TILA as to whether his failure to carry out the examination created an apparent authority in the credit card user. Instead of relying on the general law of banking which imposes on the consumer a duty to exercise care, s. 909(a) imposed on the consumer a duty to examine the account statement. The consumer performance of this rule is to be determined based on the period of 60 days from the receipt of the statement and not from the day he discovered the unauthorised payment in the statement of account.<sup>59</sup>

The consumer's duty to examine the statement of account and to notify the issuer of any unauthorised EFT payment that the consumer found there, served to protect the consumer against being made liable for the fraudulent payment losses not involving the misuse or the loss or theft of the access devices. Therefore, in the case where the unauthorised EFT transfer was initiated with the debit card details, for instance, while the card is still with the consumer, he was liable for all the losses that occurred after the lapse of the 60 days from the date he received the statement which contained the other unauthorised payments.

In conclusion, it should be noted that the *DBI* and the *Carrier* cases have settled the differences concerning the consumer's duty to give notification under s. 133(a)(1)(E) of the TILA. Based on these two cases, it is now clear that the consumer's failure to examine the statement of account is not prima facie proof of his liability for the payment

---

<sup>59</sup> *Kruser v. Bank of America* 230 Cal.App.3d 741, 281 Cal.Rptr. 463 Cal.App. 5 Dist.,1991.

initiated by another person, on the basis that the person is apparently authorised to use the consumer's credit card.

However, it is still uncertain whether the definition of unauthorised payment includes payment made by a person who misused the credit card. Moreover, it is also unclear on whom the consumer should give notice to terminate the authority of a person to initiate payment from the consumer's account. The cases discussed earlier did not provide conclusive answers to these issues. Accordingly, the consumer is left uncertain as to the mode of limiting his liability for the act of another person whose actual authority was terminated but who continues to possess the access device to the consumer's credit card account. Moreover, the decisions also showed that the TILA loss allocation rules left the consumer with the task of sorting through the facts of his relationship with the merchant and the issuer to determine the person who should be given notice to terminate the authority of the credit card's user.

### **3 THE MANDATE RULES IN THE UNITED KINGDOM**

The loss allocation scheme which defines the scope of and the conditions for the consumer's liability for unauthorised credit card, charge card and EFT payment in the United Kingdom also incorporate agency rules. This is evidenced by the reference in the

CCA and the DSRs of unauthorised payment as a payment initiated by a person who was “not acting or to be treated as acting” as an agent to the consumer.<sup>60</sup>

According to Halsbury’s Laws of England, a “person not acting” is a person who does not possess an actual authority, implied or expressed, to use the credit facility, while a “person not to be treated as agent” is a person who does not possess apparent authority.<sup>61</sup> Based on this interpretation, it is believed that the validity of the card payment has to be determined by examining the authority of the person who initiated the payment.

On the other hand, the Banking Code does not contain any specific reference to agency rules. Rather, it indirectly refers to unauthorised payment as a payment that occurs when the user obtained the card because of loss or theft.<sup>62</sup> Section 12.12 of the Banking Code also says that unauthorised payment occurs when the PIN is known by the card’s user. Since a voluntary disclosure of the PIN will make the use of the PIN a legal use, this section must refer to an involuntary transfer of the PIN. On the other hand, if the mode of access was the card details, unauthorised payment occurs if the details were used without permission from the consumer.<sup>63</sup>

---

<sup>60</sup> Section 83 (1) of the CCA and Reg. 21(1) of the DSRs.

<sup>61</sup> *Halsbury’s Laws of England*, 4<sup>th</sup> Edn Reissue (2006) 1(2) at para 29. Goode R. M. *Consumer Credit Law and Practice*, Issue 6, para 29. Apparent authority is “...the authority of the agent as it appears to others.” *per* Denning L.J in *Hely-Hutchinson v Brayhead* [1968] 1 QB 549 at 583. See Reynolds, F. M. B., *Bowstead and Reynolds on Agency*), §§ 3-005, 8-018, Gloag, W. M., *The Law of Contract: A Treatise on The Principles of Contract in The Law of Scotland*, 2<sup>nd</sup> Edn (1985), Caledonian Books, at 147-153, (Hereafter Gloag, W. M., *The Law of Contract*) and Brown, I., “The Significance of General and Special Authority in the Development of the Agent’s External Authority in English Law”, (2004) *J.B.L.* 391.

<sup>62</sup> Section 12.12 of the Code.

<sup>63</sup> *Ibid.*



The Banking Code's lack of reference to agency rules, however, does not mean that its loss allocation rules do not use the mandate rules to allocate unauthorised payment losses. In fact, s. 12.12 reference to "lost or theft" of the card, and also the use of the card details "without ... permission" indicates the application of the mandate rules in its loss allocation scheme. Accordingly, the consumer's liability for unauthorised payment should also be determined by examining the authority of the person who initiated the disputed payment.

The Banking Code loss allocation rule was applied by the Ombudsman in its decision involving a Mrs A who disputed the transactions initiated with her credit card and PIN.<sup>64</sup> The issuer claimed that by keeping the card together with the PIN in a drawer, Mrs A was grossly negligent. Accordingly she should be responsible for the transactions. Although the main issue was not whether the payment was authorised but whether the consumer was liable on the grounds of gross negligence, it should be noted that under the Banking Code, the issuer can claim that the disputed payment was facilitated by the consumer's negligence only when the payment was made without the consumer's consent. If the payment was authorised, negligence is irrelevant. Therefore, it should be noted that even if a family member used the access device, as was the case in Mrs A's problem, the payment was unauthorised if the access device was obtained without the consumer's consent.

---

<sup>64</sup> Ombudsman News at <[http://www.financial-ombudsman.org.uk/publications/ombudsman-news/46/46\\_plastic\\_cards.htm](http://www.financial-ombudsman.org.uk/publications/ombudsman-news/46/46_plastic_cards.htm)> (Visited 12<sup>th</sup> January 2006).

## **A      Unauthorised Credit Card and EFT Payment and Actual Authority**

In *Freeman & Lockyer v Buckhurst Park Properties (Mangal) Ltd* <sup>65</sup> actual authority was described as “a legal relationship between principal and agent created by a consensual agreement to which they alone are parties. Its scope is to be ascertained by applying ordinary principles of construction of contracts, including any proper implications from the express words used, the usages of the trade, or the course of business between the parties.”

Based on the above discussion apparently, there are two ways for a person to have the actual authority to initiate a credit card or an EFT payment from a consumer’s account:

### *(a)      Transfer of the consumer’s card and/or the PIN to the user*

A consumer may give the access device to his credit card or EFT account for a limited or unlimited transaction to another person. By doing that he has given the user the actual authority to initiate a payment using that device. This rule corresponds to the traditional mandate rule which authorised the bank to debit the payment to the consumer’s account if the payment was made upon the consumer’s instruction.

---

<sup>65</sup> [1964] 2 Q.B. 480 at 502, *per* Diplock L.J.

The rule was applied in a case involving one Mr B who had given his credit card and also the associated PIN to his mother for her use on holiday abroad.<sup>66</sup> Mr B disputed a transaction which he claimed was not made by his mother. However, based on the facts of the complaint, the Ombudsman found the transaction authorised.

In the above case, Mr B's act of giving his credit card to his mother falls within the rule in s. 84(2) of the CCA which allowed the issuer to allocate the whole amount of the payment to the consumer. A similar method of creating agency by actual authority should also apply to a debit card or charge card since the Banking Code scope of unauthorised payment also refers to the situation where the access device, the PIN or the card details were used without the consumer's consent.<sup>67</sup>

It should be noted that not all acts of transferring the card to another individual amount to authorising him to initiate the payment. In some cases, the merchant's terminal may have yet to be upgraded to accept PIN authentication. Therefore, the consumer may have to hand over his card to be swiped at the terminal to make the necessary payment. In this circumstance, the transfer of the card to the merchant's employee, however, did not clothe him with actual authority to make a payment from the consumer's account but only to facilitate the consumer in making the payment. Accordingly, any payment which is not requested by the consumer becomes an unauthorised payment.

---

<sup>66</sup> Ombudsman News Issue 46, at <[http://www.financial-ombudsman.org.uk/publications/ombudsman-news/46/46\\_plastic\\_cards.htm](http://www.financial-ombudsman.org.uk/publications/ombudsman-news/46/46_plastic_cards.htm)> (1<sup>st</sup> January 2006). See also case no 46/3.

<sup>67</sup> Section 12.12 of the Banking Code 2005.

This type of scenario is found in the Ombudsman's decision no 26/4.<sup>68</sup> A consumer disputed credit card transactions made at a nightclub in a foreign country while he was on holiday. Evidence showed that the authorisation codes were not in the approved format and did not conform to the numbers on the sale slips. Moreover, the merchant's credit card records, which showed a series of transactions, indicated as if the consumer was the only one paying by credit card that night. This fact raised doubt as to whether the transactions were authorised, unless it was possible to assume that the consumer had made ten separate transactions. Because there was insufficient evidence of the presence of a valid payment mandate, the ombudsman decided that the consumer was not responsible for the transactions made with his credit card.

A similar conclusion can also be found if the disputed transaction involves a debit or a charge card because the Banking Code also based the allocation of the losses on the authority of the person to initiate the disputed payment.

*(b) Additional card holder and actual authority*

Apart from the transfer of the consumer's own card, a consumer is also responsible for the payment initiated by a person to whom the issuer, with the consumer's consent,

---

<sup>68</sup> See the Ombudsman's decision in the Financial Ombudsman News Issues 26 at <<http://www.financial-ombudsman.org.uk/publications/ombudsman.htm>> (visited 10<sup>th</sup> April 2005). It is to be noted that the Ombudsman does not cover dispute involving store card. See "FSA Guide to Making a Complaint about Financial Services", at <<http://www.fsa.gov.uk/consumer/pdfs/complaint.pdf>> at 18, (Visited 10th of April 2005).

issued an access device. A supplementary or additional card holder falls within this category of individual.

This loss allocation rule is to be deduced by reading together s. 84 (2) and s. 84 (7) of the CCA which provides that a payment made using the card which was voluntarily transferred to the user is an authorised payment made by an authorised person. In the case of the EFT payment or the charge card, the rule is to be understood by reading together s.12.11 and s.12.12 of the Code. Both sections of the Banking Code contain rules which exclude a consumer who had acted negligently or fraudulently from Code protection against fraudulent payment. Since fraud or negligence applies only as an exception to the limited or the zero liability rule in s.12.12, which, in turn, applies when there is unauthorised payment, it therefore can be assumed that a consented possession of the access device means that the possessor can initiate a valid payment from the account that is linked to the access devices.

The contract between the consumer and the issuer usually describes the rule that governs the use of the access device by an additional card holder. For example, the Royal Bank of Scotland's terms and conditions provide that the consumer is responsible for all transactions made by the additional card holder.<sup>69</sup> This type of clause will bind the

---

<sup>69</sup> Clause D 22 and D 27 of the RBS Student & Graduate Royalties accounts <[http://www.rbs.co.uk/Personal\\_Finances/Students\\_&\\_Youth/Apply/sy\\_terms.htm#d](http://www.rbs.co.uk/Personal_Finances/Students_&_Youth/Apply/sy_terms.htm#d)>. See similar term in the American Express Charge Card terms and conditions clause 8, at <<http://www10.americanexpress.com/sif/cda/page/0,164,12004,00.asp>> (Visited 10<sup>th</sup> April 2006).

consumer to the payment initiated by the additional card holder until the consumer terminates the user's authority.

It should be noted that if the additional card holder voluntarily transferred his credit card to another individual, the consumer's liability for that transaction is less than clear. According to the agency rule a principal is not bound by the act of a sub-agent unless the sub-agent was appointed with his express or implied consent.<sup>70</sup> So if the consumer can be assumed to have agreed to the additional card being used by other than the additional card holder, the consumer may be liable for the transaction initiated by that person because that person becomes a sub-agent. However, s.84 (2) of the CCA, which binds the consumer to a payment initiated by a person who obtained the card with consent, only applies when the card was given by a "debtor".<sup>71</sup> By specifically referring to a "debtor" instead of an "authorised person" who according to s. 84(7) includes the additional card holder,<sup>72</sup> s.84 (2) cannot be used to bind the consumer to a payment initiated by a person to whom the card was transferred by the additional card holder. Because the transfer by the additional card holder is not a voluntary transfer by a "debtor", the consumer cannot be made liable for the disputed payment on the ground that the card was transferred with consent.

---

<sup>70</sup> *Sampson v. Wilson* [1995] 3 W.L.R. 455, See Reynolds, F. M. B., *Bowstead and Reynolds on Agency*, Chp 5.

<sup>71</sup> Section 189 (1) of the CCA reads, "debtor" means the individual receiving credit under a consumer credit agreement or the person to whom his rights and duties under the agreement have passed by assignment or operation of law..."

<sup>72</sup> Authorised person includes the issuer and the additional cardholder. See s. 84 (7) of the CCA.

Regardless of the above argument, there is the potential to allocate the disputed payment to the consumer. A reference to the rule in s.84 (1) indicates that if the additional card ceased to be in the additional card holder's possession that payment is considered as unauthorised. This rule should be read to mean when the card is being out of the additional card holder's possession without his consent such as when the card is lost or stolen. Hence, it cannot include a voluntary transfer of the card. Therefore when the additional card holder transferred the additional card to another person the consumer is responsible for that payment because the transfer is regarded as a misuse of the card by the additional card holder.<sup>73</sup> So the reason for allocating the losses to the consumer is not because the payment was made by an authorised individual who obtained the authority from the additional card holder but because of the misuse of the card by the additional card holder.

Misuse, not like theft or loss, which involves involuntary loss of control of the credit card, can include any use of the card beyond the authority granted by the consumer. For instance, in the case of Miss M, the consumer was liable for the charges made to the additional card because her partner, the additional card holder, used the additional card even after she had terminated his authority because of the ineffectiveness of the termination.<sup>74</sup> The Ombudsman's decision shows that if the additional card holder used the card in contradiction of the consumer's authorisation, the consumer is responsible for

---

<sup>73</sup> Sayer, P. E., "Credit Cards and the Law: an Introduction", (1988) 107-108, Format Publishing.

<sup>74</sup> The Financial Ombudsman decision in the Ombudsman News issue March 2001, at <<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/3/mandates.htm>>. (Visited 29<sup>th</sup> August 2005).

all the losses until the termination of the additional card holder's authority is effective, according to s. 84 (3) and (5).

The allocation of the unauthorised credit card payment based on misuse of the access device by the additional card holder is found in the terms of many credit agreements where the issuer expressly provides that the consumer is responsible for the payment initiated with the use of the additional card, even if the consumer disapproves of the transaction.<sup>75</sup>

The same loss allocation rule is believed to be applicable to an EFT payment made using a debit card since the Banking Code does not differentiate between a principal card and an additional card. Moreover, the practices of the debit card issuer show that the payment initiated with the use of an additional card is treated as an authorised payment until the issuer receives a notice of potential misuse of the card.<sup>76</sup>

---

<sup>75</sup> See clause 3 of the Lloyds TSB Bank Credit Card Condition which provides that the consumer must pay to the issuer for the additional cardholder's transaction even when the consumer disapproved the transaction, at <<http://www.lloydstsb.com/media/lloydstsb2004/pdfs/AdvanceonlineTsCs.pdf>> and clause 6 of Barclays which provides that if the additional card was obtained with the additional cardholder's consent that payment is considered as authorized. See at <[http://www.barclaycard.co.uk/Products/Apply/tandc/student\\_graduate.html](http://www.barclaycard.co.uk/Products/Apply/tandc/student_graduate.html)> (Visited 12<sup>th</sup> April 2006).

<sup>76</sup> See for instance Clause D27 of the RBS Student and Graduate Royalties Terms and Conditions at <[http://www.rbs.co.uk/Personal\\_Finances/Students\\_&\\_Youth/Apply/sy\\_terms.htm#d](http://www.rbs.co.uk/Personal_Finances/Students_&_Youth/Apply/sy_terms.htm#d)> (Visited 12<sup>th</sup> May 2006).



## **B      Unauthorised Credit Card and EFT Payment and Apparent Authority**

Apart from the actual authority, the loss allocation rules for the credit card, debit card and charge card payment also rely on the agency rule of apparent authority.<sup>77</sup> This authority arises as a result of the consumer's conduct which made the person who issued the payment mandate appear to be an authorised agent in the eyes of the issuer.<sup>78</sup> For example, an apparent authority may be created by the consumer's failure to effectively terminate the actual authority of the person who was appointed as an additional card holder or of a person who was allowed by the consumer to use his credit card, debit card or charge card.<sup>79</sup>

The rule that binds the consumer to the payment transaction initiated by a person who possesses an apparent authority is to be understood from the notification rule in s.84 (3) of the CCA and s. 12.12 of the Banking Code. These sections provide that a consumer can limit his losses from an unauthorised payment by reporting to the issuer the event which may facilitate fraudulent payment including the loss, theft or possible misuse of the access device. Since notification to terminate the appearance of authority is necessary to limit the principals' liability for the act of a person who appeared to the

---

<sup>77</sup> Beale, H. G., *Chitty on Contracts*, at para 31-056, See *Hely Hutchinson v Brayhead Ltd* [1968] 1 Q. B. 549, and *Bank of Scotland v. Brunswick Developments* (1987) Ltd 1997 S.C. 226.

<sup>78</sup> Ibid. *Bank of Scotland v. Brunswick Developments* (1987) Ltd 1999 S.C. (H.L.) 53, and *Freeman and Lockyer v Buckhurst Park Properties (Mangal) Ltd*, [1964] 2 Q.B. 480, at 503 *per* Diplock L.J. See contrary view which maintained that the representation may come from the agent himself in *First Energy (UK) Ltd v. Hungarian International Bank Ltd*. [1993] 2 Lloyd's Rep. 194 and Reynolds, F.M.B., "The Ultimate Apparent Authority" (1994) *L.Q.R.* 110, 21-25.

<sup>79</sup> Reynolds, F. M. B., *Bowstead and Reynolds on Agency*, Chp 8.

other party in the contract to be acting with authority,<sup>80</sup> the incorporation of this rule in the CCA and the Banking Code suggests that their loss allocation schemes also incorporate the agency rule of apparent authority.

*(a) Apparent authority, notice of termination and the return of the access card.*

As mentioned earlier, when the consumer consents to the appointment of another as an additional card holder or when he gives his credit card to another, that person possesses the actual authority to initiate a credit card, debit card or charge card transaction from the consumer's account.

Consequently, when the consumer fails to effectively terminate that authority, he is bound by the payment initiated by that person. The agency rule of apparent authority was used to allocate the payment in the case of a Miss M who disputed the charges to her credit card account on the grounds of unauthorised use of the card by an additional card holder.<sup>81</sup> Miss M had nominated her partner Mr N as an additional card holder to her credit card account. After they fell out, she asked the issuer to cancel the additional card. However, Miss M failed to retrieve and return the card to the issuer as required by the credit agreement, thereby enabling Mr N to continue using the card.

---

<sup>80</sup> *Lloyds Bank Plc. v. Independent Insurance Co. Ltd.*, [2000] Q.B. 110 referring to Reynolds, F. M. B., *Bowstead and Reynolds on Agency*, § 8-009. See also Gloag, W. M., *The Law of Contract*, at 147.

<sup>81</sup> The Financial Ombudsman decision in the Ombudsman News issue March 2001, at <<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/3/mandates.htm>>. (Visited 29<sup>th</sup> August 2005).

The Ombudsman reached two different conclusions as to the disputed charges. First, the amount of charges resulting from any transaction which did not require the issuer's authorisation was to be allocated to Miss M because she had failed to return the card to the issuer as required by the credit agreement. The Ombudsman cited industry practice which set a certain minimum limit for authorisation, said that it was impossible for the merchant to know the cancellation status of the card even if the issuer had put a mark on the card, because the merchant need not contact the issuer for authorisation. However, if the payment required authorisation, the merchant could be warned by the issuer against accepting the card. Therefore, for other transactions that require authorisation, the losses would be allocated to the issuer because it had failed to set up a warning system which would have alerted the merchant to the card user's lack of authority.

The Ombudsman's decision was centred on the use of the card by the estranged partner in absence of authority. It is, however, not clear who was the third party that had relied on the payment mandate created by the use of the card; a person whose presence is essential in the creation of an apparent authority.<sup>82</sup>

The first part of the decision indicated that the merchant was the third party since the notice of termination of the user's authority was supposed to be given to the merchant. In the second part of the decision where the payment requires authorisation, the Ombudsman's decision also suggested that the merchant is the third party to whom

---

<sup>82</sup> Beale, H. G., *Chitty On Contracts*, para 31-056.

notice of the termination of the agent's apparent authority is to be given. However, instead of giving notice directly to the merchant, the consumer may give notice through the issuer who can use a particular warning system to alert the merchant to the potential unauthorised use of the card.

It should be noted that although the decision was practical as it was based on industry practices, yet it runs contrary to s. 84 (3) of the CCA which requires the notice to terminate the apparent authority of the card's user to be given to the issuer.<sup>83</sup> In particular, the language of s. 84 (3), which refers to the notice of loss or theft of the credit card, pointing to an involuntary transfer of the access device to its user, and also a notice of "misuse", indicates that there are other events that may facilitate unauthorised transactions apart from the use of a stolen or lost credit card.<sup>84</sup> Therefore, if the card was voluntarily given but was used beyond the authorised scope or limit or even after the authority was terminated, notice given by the consumer to the issuer should be sufficient to limit the consumer's losses.

In the case of Miss M, there was the potential for unauthorised payment to occur since the absconded partner was in possession of the additional card. Accordingly, the notice

---

<sup>83</sup> Section 84 (3) provides, " Subsections (1) and (2) shall not apply to any use of the credit-token after the creditor has been given oral or written notice that it is lost or stolen, or is for any other reason liable to misuse."

<sup>84</sup> Section 1(1) of the Theft Act 1968 "A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it, and 'thief' and 'steal' shall be construed accordingly." Section 3 (1) of the same Act which defined appropriation brings the act of losing the payment devices under an involuntary scope; "Any assumption by a person of the rights of an owner amounts to an appropriation, and this includes, where he has come by the property (innocently or not) without stealing it, any later assumption of a right to it by keeping or dealing with it as owner.

sent to the issuer telling it of Miss M's decision to terminate her partner's authority to use the card should have effectively terminated the partner's apparent authority and free Miss M from the losses.

The Ombudsman's decisions were influenced by the term of the credit agreement which required the consumer to return the additional card before the termination of the user's authority was made effective. However, that should not be the case because that term contradicts s. 173 (1) of the CCA which renders any provision of the credit agreement that "is inconsistent with a provision for the protection of the debtor" under the CCA void. Since inconsistency refers to any term that "purports to impose, directly or indirectly, an additional duty or liability on [the consumer] in those circumstances",<sup>85</sup> a contract term which requires the consumer to return the additional card to effectively terminate the user's authority, in fact, imposes on the consumer a duty beyond the one required by s. 84 (3) of the CCA.

Had the dispute in Miss M's case involved a debit card or a charge, the decision would also contradict s. 12.12 of the Banking Code which, similar to the rule in s. 84 (3) of the CCA, requires the consumer to notify the issuer of the potential misuse. Even if the issuer's contract term requires the consumer to return the card before the apparent authority of its holder can be effectively terminated, it is most probably unenforceable if

---

<sup>85</sup> Section 173(2) of the CCA.

the issuer promised to act fairly and reasonably in all its dealings with the consumer including to put the Code into practice.<sup>86</sup>

*(b) Apparent authority, negligence and the management of the access device*

Apart from being liable for a payment initiated by a person who possessed an apparent authority, a consumer may also be liable for an unauthorised EFT payment or charge card payment on the grounds of negligence.<sup>87</sup> Negligence prevents the consumer from denying the validity of the disputed payment because it was facilitated by his failure to exercise care.<sup>88</sup>

Originally, in a cheque payment system, the consumer has a duty to exercise reasonable care in relation to the cheque “transaction”; i.e., in the drawing and the signing of the cheque but not in the management of the cheque.<sup>89</sup> By analogy, the duty to exercise care in a debit card or a charge card payment means a duty to protect the card and /or PIN security at the time of making the transaction but not to manage their security when they are not in use.

---

<sup>86</sup> Section 2 of the Banking Code. See Cartwright, P., *Banks, Consumers and Regulations* (2004) at 125-226, Hart Publishing.

<sup>87</sup> Reynolds, F. M. B., *Bowstead and Reynolds on Agency*, § 2-099.

<sup>88</sup> Section 12.11, read together with s. 12.5 of the Banking Code. See *Tai Hing Cotton Mill Ltd. v. Liu Chong Hing Bank Ltd* [1986] A.C. 80, 101-104., and *Greenwood v Martins Bank Ltd* [1933] A.C. 51, 57. *London Joint Stock Bank v MacMillan and Arthur* [1918] A.C. 777, 835.

<sup>89</sup> Geva, B., “Allocation of Forged Cheque Losses - Comparative Aspects” (1998) *L.Q.R* 114 (Apr), 250 at 262.

If the restricted concept of the duty of care is applied to the debit card and charge card payment, the consumer is free from any responsibility for unauthorised payment caused by the loss or theft of his card even if the theft occurred before his eyes. Similarly, he is also not responsible for the losses even if he carries the card together with the PIN in his stolen wallet. The reason is because in both scenarios, the carelessness was in the management of the card and the PIN and not in the card transaction through the use of his card and/or PIN.

However, it is believed that the above duty, which was founded in the *London Joint Stock Bank v MacMillan and Arthur*<sup>90</sup> and later confirmed in the *Tai Hing Cotton Mill Ltd. v. Liu Chong Hing Bank Ltd's*<sup>91</sup> case, was expanded by the Banking Code loss allocation rules. Section 12.5 of the Code allows the issuer to impose on the consumer via the contract terms, the duty to exercise care with regard to both the transaction and the management of the card and the PIN.<sup>92</sup>

The negligence-based loss allocation rule was applied by the Ombudsman in its decision no 09/09, when it allocated the losses that resulted from unauthorised use of a cash card by a thief to a consumer who kept a note of the PIN, together with the card.<sup>93</sup> In this

---

<sup>90</sup> [1918] A.C. 777.

<sup>91</sup> [1986] A.C. 80.

<sup>92</sup> See for example clause 6 of the Cooperative Bank Current Account Terms and Conditions at <<http://www.co-operativebank.co.uk/servlet/Satellite?cid=1076405704423&pagename=CoopBank%2FPage%2FtplPageStandard&c=Page>> and clause 9.3 of the HSBC Personal Banking Terms and Conditions at <[http://www.hhsbc.co.uk/1/PA\\_1\\_4\\_24P/content/uk/pdfs/en/personal\\_banking\\_terms.pdf](http://www.hhsbc.co.uk/1/PA_1_4_24P/content/uk/pdfs/en/personal_banking_terms.pdf)> (Visited 12<sup>th</sup> June 2005).

<sup>93</sup> See the Ombudsman's decision at <<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/9/sept-disputed-cash-machine-withdrawals.htm>> (Visited 29<sup>th</sup> August 2005).

case, Mr T's wallet was stolen. He forgot to inform the issuer of the loss of his cash card though he reported the loss of other cards. It emerged that Mr T kept the cash card and a poorly disguised PIN together in the stolen wallet. Because Mr T's act of keeping the poorly disguised PIN and card together contradicts the terms of the contract, and is therefore negligent by virtue of the Code, the whole losses are his.

The duty to exercise care in relation to the security of the access device is presumably applicable to a payment made in a distance transaction via a distance communication system such as internet or mobile commerce systems. This is to be observed from the rule in Reg. 21(1) of the DSRs which protects the consumer against fraudulent card payment made in a distance transaction when the person who initiated the payment did not possess actual or an apparent authority. Presumably, since payment in a distance transaction can be initiated by using the card or the account details, the consumer's failure to exercise care in relation to the security of the card allowing another to use the details may exclude him from the DSRs protection. This effect is to be understood by reading s.12.12 of the Banking Code, together with s.12.11 and 12.5 which shows that the consumer's failure to protect the safety of the account details is negligence that voids the DSRs and the Banking Code zero liability protection.

The duty to exercise care, however, does not apply to the credit card payment because s.173 of the CCA expressly invalidates any contract terms that contradict the protection given by the CCA to the consumer. Accordingly, negligence-based loss allocation rules



do not apply in relation to credit card payment because they are not part of the CCA loss allocation scheme.

The effect of s. 173 of the CCA can be seen in the Ombudsman's decision no. 25/13.<sup>94</sup>

In this case, a dispute occurred over unauthorised withdrawals made with the consumer's cash card which had effectively increased the consumer's credit with the issuer. The issuer argued that because the correct PIN was used for each withdrawal, the consumer must have acted negligently in keeping the PIN and the card together.

The Ombudsman nevertheless rejected the issuer's argument. It went on to explain the scope of the CCA in relation to the negligence loss allocation rule and said that although the unauthorised withdrawals increased the consumer's credit with the issuer, thereby changing the card into a credit token within the CCA, yet the consumer's liability for the unauthorised payment was not to be assessed on the grounds of negligence but according to the rule in s. 84(1) and (2) of the CCA. Accordingly, the consumer's liability is caps at £50 regardless of his negligence, provided he informs the issuer of the loss or theft of his credit card.

Apart from the duty to exercise care in relation to the security of access devices, it is uncertain whether the consumer's delay in giving notice under s. 12.12 is also considered as negligence. Apparently, this section did not specify the time frame for notification, suggesting that the consumer may give to the issuer notice of loss or theft or

---

<sup>94</sup> The Ombudsman News at <<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/25/25-banking-disputed-cash-withdrawals.htm>> See other cases in Ombudsman New issue 44 at <[http://www.financial-ombudsman.org.uk/publications/ombudsman-news/44/44\\_banking\\_case.htm](http://www.financial-ombudsman.org.uk/publications/ombudsman-news/44/44_banking_case.htm)> (Visited 12<sup>th</sup> April 2006).

other events that may facilitate fraud at anytime he wishes, similar to the position under s. 84 (3) of the CCA. However, since the rule in s. 12.11 refers to negligence as to include failure to comply with the contract terms, it indicates that if the losses were caused by the delay in notification, and that delay happened because the consumer failed to adhere to the timeframe provided in the contract, the consumer might be liable for all the losses that would ensue from that failure. Hence, when a contract requires notice to be given within a specific period, the consumer must give timely notice to avoid losses. This is so because a failure to give notice will prevent the consumer from denying the authority of the person who initiated the disputed payment.<sup>95</sup>

The effect of that term on the consumer may be observed from the Ombudsman's decision no. 09/10 which involved the theft of a cash card.<sup>96</sup> The consumer telephoned the issuer almost immediately after realising that her handbag, which contained her card and PIN, was stolen. However, the issuer disputed this fact and claimed that the withdrawals were made before it was informed of the theft. The Ombudsman upheld the consumer's complaint because the issuer failed to prove his claim. Probably had the issuer succeeded in proving that the notice was given after the withdrawals, the consumer would have been liable for all the losses.

---

<sup>95</sup> For example, clause 2.2 of the First Trust Bank Visa Debit Card Terms and Conditions required the consumer to give the notice "as soon as possible", while clause 6.5 of the Cooperative Bank Cashminder Account & Electron Debit Card Terms and Conditions required the consumer to give the notice "immediately".

<sup>96</sup> See the Ombudsman's decision no 09/10 at <<http://www.financial-ombudsman.org.uk/publications/Ombudsman-news/9/sept-disputed-cash-machine-withdrawals.htm>> (Visited 29<sup>th</sup> August 2005).

The Ombudsman's concern with the issuer's onus to prove that the consumer had delayed notifying the theft of her card and PIN, indicates that the contract term may subject the consumer to a duty to exercise care with regard to the time of notification.

*(c) Apparent authority, negligence and the duty to examine the statement of account.*

Basically, a consumer is not under a duty to examine his statement of account.<sup>97</sup> However, if he examines the statement and discovers an unauthorised payment, he has a duty to inform the issuer of that transaction.<sup>98</sup> The duty to disclose, which is known as the Greenwood duty, after the case of *Greenwood v Martin Bank*,<sup>99</sup> is formed when the consumer possesses actual knowledge of the unauthorised transaction and must not be based on constructive knowledge.<sup>100</sup> It means that the consumer must have found the transaction in the account statement. However, if he receives the statement but does not check it, and does not find the fraudulent payment, he is not responsible for that transaction and any other that occurs thereafter.

The duty to examine the statement of account, does not apply to the additional cardholder because the contract is in the name of the consumer and the statement is therefore addressed and sent to the consumer. Thus, if the additional card holder knows

---

<sup>97</sup> *Tai Hing Cotton Mill Ltd. Appellant v. Liu Chong Hing Bank Ltd* [1986] A.C. 80, at 106. See clause 1.7 of the Cooperative Bank and clause 2.3 the HSBC terms and conditions, *supra* n 92.

<sup>98</sup> *Ibid.*

<sup>99</sup> *Greenwood v Martin Bank* [1933] A.C. 51, at 57-58.

<sup>100</sup> In *Patel and others v Standard Chartered Bank*, [2001] All ER (D) 66, at para 65, the court rejected the proposition that the accountholder owes a duty to notify the bank of the cheque forgery upon constructive knowledge of that forgery.

about an unauthorised payment initiated with the additional card, he is not responsible to give notice of the payment to the issuer. Nonetheless, if he informs the issuer, the notice should be sufficient to protect the consumer from the unauthorised payment losses.

Although the consumer is not under a duty to examine the account statement the issuer may impose that duty on the consumer via its contract terms. If that is the case, the consumer's failure to comply with the term constitutes negligence under s.12.11 of the Banking Code.<sup>101</sup> As such, the consumer cannot deny the validity of the disputed payment because his negligence manifested the presence of the card user's authority.<sup>102</sup>

The consumer's failure to report any unauthorised transaction found in the statement of account to the issuer may also invalidate the protection given under Reg. 21(1) of the DSRs when the unauthorised debit card or charge card payment has been made in a distance transaction. Although the DSRs do not qualify the protection given by Reg. 21 by a negligence rule, they also apply the agency rule of apparent authority in their loss allocation scheme.<sup>103</sup> As a result, the consumer may not claim the zero liability protection of the DSRs because his failure to inform the issuer of an unauthorised payment that is recorded in the statement of account while still having the card in his possession, may constitute negligence which consequently, would created apparent authority by *estoppel*.

---

<sup>101</sup> *Tai Hing Cotton Mill Ltd. Appellant v. Liu Chong Hing Bank Ltd* [1986] A.C. 80, at 106. See clause 1.7 of the Cooperative Bank and clause 2.3 the HSBC terms and conditions, *supra* n 91.

<sup>102</sup> *Supra* n 87 and n 88.

<sup>103</sup> See page 96.

In conclusion, the mandate rules as applied in the credit card payment system differ from the one applicable in the EFT and the charge card payment systems. In the credit card payment systems, the statutory loss allocation scheme provided by the CCA applies common law agency rules. The CCA does not allocate losses based on negligence. Hence, apparent authority by *estoppel*, created as a result of the consumer's negligence, does not play any role in the allocation of losses caused by fraudulent credit card payment. The said rule, however, is used by the Banking Code loss allocation scheme. Therefore, the issuer may choose to allocate the losses caused by fraudulent debit card or charge card payments based on apparent authority by *estoppel* apart from actual authority.

However, regardless of the differences, credit card, debit card and charge card loss allocation rules share a common trait when it comes to the limit of the consumer's liability for unauthorised payment because both the CCA and the Banking Code cap the amount of losses to be allocated to the consumer at £50. Moreover, the consumer in all three systems is protected from unauthorised distance payment by virtue of Reg. 21 of the DSRs.

Finally, the CCA and the Banking Code loss allocation schemes rely on notification of events that may facilitate fraudulent payment as a basis for allocating fraudulent payment losses. However, the failure to give timely notice differs because the Banking Code allows the issuer to fix a time frame for notification via its contract terms whereby failure of compliance constitutes negligence. On the other hand, the CCA does not fix a

time for notification. Therefore, the consumer may give notice to terminate the authority of the card user any time he wishes and still be protected by the capped liability limit of £50.00.

#### **4 THE MANDATE RULES IN MALAYSIA**

it should be noted that the CC and EFT Guidelines, which, respectively, govern the allocation of fraudulent payment losses in the credit card and EFT payment systems, do not have any direct reference to mandate rules in their loss allocation schemes. Nevertheless, looking at their rules which assess the consumer's liability by examining the presence and absence of an authority of the person who issued the payment mandate, and the nature of the relationship between the consumer and the issuer, which is of agent and principal, it can be deduced that the loss allocation rules in these two Guidelines also incorporate the mandate rules.<sup>104</sup>

Accordingly, the consumer's liability for fraudulent payment losses would also require an examination of the authority of the person who initiated the payment from the consumer's credit card or EFT account. The authority includes actual authority and apparent authority.

---

<sup>104</sup> Lee, M. P., *Banking* (1995), 3.2, Butterworths Asia. See *Perdana Merchants Bankers Bhd (Previously known as Intradagang Merchant Banking (M) Bhd) v Abdul Rahim Bin Abdul Hamid & Ors* [2001] 2 MLJ 711, at 727-728 and *Hop See Sen & Anor v Public Bank* [1988] 2 MLJ 170.

The one and only case that may explain the concept of unauthorised credit card payment is the case of *Bakmawar Sdn Bhd v Malayan Banking Bhd*.<sup>105</sup> In this case, the dispute involved the defendant's right to charge back the plaintiff's merchant account with unauthorised credit card payments under the merchant agreement when two card holders disputed the validity of the transactions initiated with the use of their credit cards at one of the plaintiff's outlets. The plaintiff claimed that the charge back was unauthorised and unlawful under the terms of the merchant agreement.<sup>106</sup> The plaintiff did not dispute the fact that unauthorised credit card payments had occurred but argued that clause 10 (g) of the merchant agreement, which allows the issuer to exercise chargeback when the credit card was used to finance transaction in violation of the law, does not cover cases of fraudulent payment.

The court, however, decided that unauthorised use of the credit card constituted 'fraud' as a form of a violation of the law that falls within clause 10 (g) of the merchant agreement. It should be noted that even though the judge did not explain in detail the concept of unauthorised credit card payment; which would be very helpful in interpreting the rule in the CC Guidelines, yet it can be established from clause 10 (c) of the merchant agreement and also from the judge's definition of fraud "as a form of a

---

<sup>105</sup> [1992] 1 MLJ 67, at 71.

<sup>106</sup> Clause 10 reads as follows:

Merchant agrees to pay bank the total face amount of any sales draft, and bank will have the right at any time to charge merchant's commercial account therefor without notice, in any situation relating to such sales drafts where:

(c) the sales draft is alleged to have been drawn improperly or without authority.

(e) the cardholder disputes the sale, quality, or delivery of merchandise or the performance or quality of services covered by the sales draft.

(g) sale of merchandise, performance of services, or use of a Malayan Banking Card thereof involves a violation of law or the rules or regulations of any governmental agency or otherwise.

violation of the law” that unauthorised credit card payment covers a situation where the person who used the card did not have authority to do so.<sup>107</sup>

## **A      Unauthorised Credit Card and EFT Payment and Actual Authority**

In Malaysia, actual authority has the same meaning as given by Diplock L.J in *Freeman and Lockyer v Buckhurst Park Properties (Mangal) Ltd*<sup>108</sup> that is, it is a legal relationship which is based on a consensual agreement between the principal and agent.<sup>109</sup> Accordingly, when considering the consumer’s liability for a credit card or an EFT payment, it is necessary to determine the authority of the person who initiated the respective payment.

An agent’s actual authority can be expressly given or implied from the surrounding circumstances.<sup>110</sup> Therefore, a consumer is bound by a credit card or EFT payment made by the issuer upon receiving a mandate issued by a person who received the access devices and /or the access code with the consumer’s consent. The voluntary transfer of the mode of accessing the consumer’s account may involve either of the following:

---

<sup>107</sup> Supra n 105, at 71.

<sup>108</sup> [1964] 1 All ER 630, at 644.

<sup>109</sup> *Mahfuz Bin Hashim v Koperasi Pekebun Kecil Daerah Segamat & Ors*[2005] 3 MLJ 726.

<sup>110</sup> See s.139 and s. 140 of the Malaysian Contract Act 1950 (Revised 1973). (Hereafter the Contract Act).



*(a) Transfer of the consumer's access device and/or code to the user*

As mentioned, the CC and EFT Guidelines do not directly allocate the losses by specific reference to actual authority. However, the rule in Para 13.2 of the CC Guidelines, which is applicable to the credit card payment, provides that a consumer is not liable for “unauthorised transactions” as a consequence of loss or theft of a credit card except to the maximum amount of RM250.<sup>111</sup> This rule indicates that an unauthorised credit card transaction occurs when the person who initiated the payment obtained the card as a result of “loss” or “theft” of the card.

A similar approach is found in the EFT Guidelines which are applicable to an EFT payment. Paragraph 13.3 of the EFT Guidelines refers to unauthorised payment as a payment that was made when there is a lost or stolen card or when the access code security has been breached.

By referring to loss<sup>112</sup> and theft<sup>113</sup> of the card the rules in both Guidelines indirectly point to unauthorised credit card or EFT transactions that occur when an access device was involuntarily transferred from the consumer's possession to the user. In other words, when the user, without the consumer's consent, obtains an access device, the

---

<sup>111</sup> At the exchange rate of 7.00 the amount would be £36.00 approximately

<sup>112</sup> In *Kedai Pajak Fah Ngien & Ors V Public Prosecutor* [2002] 5 MLJ 613, at 622 it was explained that lost occurred when the owner is deprived of an article without his voluntary action, conduct or prior knowledge.

<sup>113</sup> In *Shamsudin Bin Shaik Jamaludin v Kenwood Electronics Technologies (M) Sdn Bhd* [1999] 3 MLJ 438. at 477 the court held that to constitute theft under s.378 of the Malaysian Penal Code two elements must be proved, first “moving a moveable property of a person out of his possession without his consent”, and second “the moving [is intended to take] the moveable property with a dishonest intention.”

payment initiated with it is unauthorised because that person did not possess an actual authority.<sup>114</sup> Accordingly, the consumer is not bound by the payment made by the issuer upon receiving the unauthorised payment mandate. This rule is based on the principle that when the issuer, who is an agent of the consumer in making the necessary payment to the payee acted outside the consumer's mandate, the consumer is not bound to that act.<sup>115</sup>

Despite the above similarity, the EFT Guidelines loss allocation scheme is wider in scope than the CC Guidelines since it also covers unauthorised payment initiated by a person who obtained the access code; which includes the intangible means of accessing the account such as a PIN and code, without the consumer's consent because of a code security breach.<sup>116</sup>

It should be noted that though Para 15 (3) does not give a detailed explanation of the circumstances that constitutes security breach, it is believed that based on the use of computer technology in the EFT payment systems and the definition of the access code which refers to PIN, passwords or codes that enable the user to access the consumer's account via electronic systems, breach of an access code may refer to an act which

---

<sup>114</sup> See the decision in *Woodland Development Sdn Bhd v Chartered Bank; PJTV & Densun (M) Sdn Bhd (Third Party)* [1986] 1 MLJ 84, at 89 where the court relied on the definition of agent's authority given in the English decision of *Freeman and Lockyer v Buckhurst Park Properties (Mangal) Limited* [1964] 2 QB 480. See also the definition of actual, express and implied authority in s.139 through s.141 of the Malaysian Contract Act 1950.

<sup>115</sup> Section 175 of the Contracts Act. See *Tan Tian Quee v Kuppusamy* [1967] 2 MLJ 66.

<sup>116</sup> Paragraph 15 and Para 3 of the EFT Guidelines.

constitutes a crime of unauthorised access to a computer under s. 3 of the Computer Crime Act 1997.<sup>117</sup>

Again, it can be seen that in the case of unauthorised access, as a result of a security breach, there is a lack of a consumer's consent to the use of the access code. This suggests that when the access code was voluntarily transferred to the user, the consumer is liable for the payment because the user had initiated the payment while having an actual authority to use the code.

*(b) Additional card holder and actual authority*

When a person is appointed as an additional credit card or debit card holder and is given an access device and/or code, the payment initiated using that mode of access falls within the category of an authorised payment. However, neither the CC nor EFT Guidelines contain any reference to a payment initiated by an additional card holder. However, since it is common for an account holder to require the bank to issue an additional card to another person, it is believed that any payment initiated by that person with the use of that additional card falls within the category of authorised payment.<sup>118</sup>

---

<sup>117</sup> Section 3. Unauthorized access to computer material

(1) A person shall be guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorized; and

(c) he knows at the time when he causes the computer to perform the function that is the case.

Section 2(1) defined computer to include any computerised system that can store; process; display and communicate data.

<sup>118</sup> See for example Clause 9 of Maybank Gold Credit Card terms and conditions at <<http://www.maybank>

The payment binds the consumer to the issuer by virtue of the agreement entered into between the consumer and the issuer irrespective of the value and the purpose of the payment until the authority to access the account is terminated or revoked.

Despite the issuer's common practice of issuing the additional card, neither the CC nor EFT Guidelines address the issue of the misuse of an additional card by an additional card holder. Nevertheless, from the language of the CC Guidelines which capped consumer liability for fraudulent payment losses only when the access device was obtained as a result of loss or theft,<sup>119</sup> it is believed that the consumer is responsible for the credit card payment initiated by a person to whom the additional card was voluntarily transferred by the additional card holder because the user possessed actual authority to use the card.

In so far as the EFT payment is concerned, the EFT Guidelines provide in Para 15(3) that the consumer's liability may be capped if the issuer is informed of the misuse of the card. This expanded duty of notification is to be inferred from the language of Para 15 (3) which refers to notification of the card which is "lost" and "stolen" and also "misused". While loss and theft refer to involuntary transfer of the card's control from the consumer to the user,<sup>120</sup> the term "misused" may be interpreted to refer to the situation where the card is voluntarily transferred to the user but it is beyond the authorised limit or purpose.

---

[2u.com.my/consumer/online\\_cards/agreement\\_gold.pdf](http://2u.com.my/consumer/online_cards/agreement_gold.pdf)> (Visited 12<sup>th</sup> May 2006).

<sup>119</sup> Paragraph 13.2 of the CC Guidelines.

<sup>120</sup> See page 121 and notes 112 and 113.

This rule indicates that the consumer may be liable for the misuse of the debit card by the additional card holder including when there is a transfer of the additional card to another person until the issuer is informed of the misuse.

## **B      Unauthorised Credit Card and EFT Payment and Apparent Authority**

Apart from an actual authority, both the CC and EFT Guidelines also incorporate the agency rule of apparent authority to assess the validity of a payment made by the issuer on behalf of the consumer. Apparent authority is defined by s. 190 of the Contract Act as an authority that is created by the act or words of the principal which causes a third party dealing with the agent to believe that the agent is authorised to act.<sup>121</sup> Accordingly, if the person who issued the payment mandate is proven to possess this type of authority, the consumer is responsible for the disputed payment.

There is no direct reference to apparent authority just like there is no reference to actual authority in the CC Guidelines loss allocation scheme. However, the apparent authority rule can be deduced from Para 13.2 of the CC Guidelines which requires the consumer to notify the issuer of loss or theft of the credit card before he can claim the Guidelines' protection against fraudulent payment losses. A similar deduction can also be made in the case of the EFT payment since Para 15.3 of the EFT Guidelines also requires a

---

<sup>121</sup> Section 190 of the Contract Act provides: "When an agent has, without authority, done acts or incurred obligations to third persons on behalf of his principal, the principal is bound by those acts or obligations if he has by words or conduct induced such third persons to believe that those acts and obligations were within the scope of the agent's authority." See *MMC Power Sdn Bhd & Anor v Abdul Fattah B Mogawan & Anor* [2001] 1 MLJ 169, at 174.

notification of similar events with additional notice of misuse of the card or breach of the access code security. A notification to limit one's responsibility for the act of another with a third person is a trait of the agency rules.<sup>122</sup> Therefore, when both Guidelines require notification in order to protect the consumer from further fraudulent payment, it can be assumed that agency by apparent authority is applicable in the allocation of credit card and EFT fraudulent payment losses.

Accordingly, any payment initiated after the required notice was given to the issuer should not bind the consumer because the notification eliminates the appearance of authority.<sup>123</sup> Equally, the consumer's failure to give the required notice may prevent him from denying the authority of the person who initiated the payment because the issuer had changed his position by making the payment, in reliance on the appearance of the authority of the person who used the credit card or the debit card.<sup>124</sup>

*(a) Apparent authority, notice of termination of authority and the return of the card to the issuer*

Paragraph 13.2 of the CC Guidelines provides that unauthorised credit card payment, -

---

<sup>122</sup> See s. 161 of the Contract Act which provides that the authority is terminated by giving a notice to that effect to the third party who deals with the agent.

<sup>123</sup> Section 154 – s.161 of the Contract Act. See *MMC Power Sdn Bhd & Anor v Abdul Fattah B Mogawan & Anor* [2001] 1 MLJ 169.

<sup>124</sup> See *SPH De Silva v Is David* [1972] 2 MLJ 22, at 24. See Vohrah, B., and Wu, M. A., *The Commercial Law of Malaysia*, 2<sup>nd</sup> Edn. (2003) 388, Longman. (Hereafter Vohrah, B. and Wu, M. A., *The Commercial law of Malaysia*)

which occurred as a consequence of loss or theft of a credit card is to be allocated to the issuer if the payment was made after the consumer had informed the issuer of the loss or theft.

The language of this provision shows that the consumer is protected against payment initiated by unauthorised individuals. It also shows that notification to terminate the apparent authority of a person to initiate a credit card payment can only work if the card is lost or stolen. However, the rule cannot be extended to protect the consumer against a payment initiated by an authorised person who misused the card since in that circumstance, the card is not lost or stolen. The limited scope of the rule in Para 13.2 of the CC Guidelines means that the consumer is not entitled to the protection of the capped liability limit even if he had given the issuer notice informing of his intention to terminate the card holder's authority.

Paragraph 13.1 which requires the issuer to provide an "effective and convenient means" of notification of "any loss[s], theft or unauthorised use" of the credit card, indicates that unauthorised payment may occur even if the credit card is not lost or stolen. Accordingly, if the rule is read on its own, it means that a consumer can give notice to limit his liability from misuse of the credit card by an authorised individual. Nevertheless, reading both the rule in 13.1 and 13.2 it appears that only notice of loss or theft of the card can effectively limit the consumer's losses. Therefore, it is not an overstatement to suggest that although the credit agreement may require the consumer to inform the issuer of the potential misuse of the credit card, the issuer may, at the same

time, allocate all the losses to the consumer, irrespective of the capped liability limit in Para 13.2.

Furthermore, since the rules in Para 13.1 and 13.2 only refer to payment initiated using the card, the consumer cannot stop the misuse of the card details unless the card is lost or stolen. In the case where the card is not lost or stolen, the consumer also cannot give a notice of misuse of card details to limit his losses from any unauthorised payment initiated using the card details unless, as suggested, the details are obtained from a lost or stolen card.<sup>125</sup> Consequently, the issuer may allocate to the consumer all the losses caused by fraudulent use of the card details obtained from sources other than a stolen or lost credit card.

Similar to the CC Guidelines, the EFTA Guidelines also allocate the losses from any unauthorised debit card payment to the consumer when the payment has been made by a person who possessed an apparent authority to use the consumer's debit card or access code unless the issuer was informed of the termination of that authority beforehand.

Despite the similarity, the notification rule in Para 15 (3) of the EFT Guidelines is wider as it also applies to the case of misuse of the debit card by a person whose authority has been terminated or is limited in scope.<sup>126</sup> Therefore, the issuer may allocate to the consumer all the losses caused by misuse of the card if the consumer failed to inform the

---

<sup>125</sup> See Chapter two at 60-61.

<sup>126</sup> See above pages 61 and 124.



issuer of the card's misuse because that failure made the card user appear to be authorised to initiate the payment. Accordingly, it is necessary for the consumer to give notice to terminate the apparent authority of the card's user so that his losses can be limited to the actual losses incurred before the notification.<sup>127</sup> The misuse of the card rule should also apply when the additional card holder gives the additional card to another person.

Another scenario where an unauthorised debit card payment can be allocated to the consumer on the grounds of apparent authority, is when the consumer fails to inform the issuer that his access code security has been breached. This rule is to be found by reading together Para 15 (3) and Para 16 of the EFT Guidelines which clearly link the liability of the consumer to the necessity to notify of an access code security breach.

As tracing an access code security breach is not as easy as checking a wallet to ensure that the debit card is not missing, there is uncertainty as to the circumstances in which notification should be made by the consumer. Moreover, unless the consumer diligently checks his statement of account, it is hard to imagine a situation where the consumer would know about that security breach, especially if the card is still in his possession.

Perhaps a solution can be found by reading together Para 14(1), Para 15.3, and Para 16 of the EFT Guidelines, which require the consumer to examine his statement of account

---

<sup>127</sup> Paragraph 15.3 and Para 16 (a) and (b) of the EFT Guidelines. Compare them to s. 84 (3) of the CCA which requires notice in a situation where the card "is liable for misuse".

and to inform the issuer of any unauthorised payment that he finds without delay. However, the combined effect of these provisions do not take us very far because Para 14 does not explain the consequence of a failure to perform this duty.

Moreover, a combined reading of these provisions also affects the protection of the consumer against unauthorised payment. In particular, Para 14 (2) requires the consumer to inform the issuer of any unauthorised transaction that is recorded in the statement of account within 60 days from the date of the statement. It means that if the consumer is not in the habit of examining the statement of account, the notification period may have elapsed by the time he discovers unauthorised payments facilitated by a breach of the access code security. Worst of all, this delay may fall within the scope of Para 16, which allows the issuer to allocate to the consumer all the losses from the unauthorised use of the consumer's access code.

Based on the above discussion, it is believed that the EFT Guidelines' rule on giving notice of a breach of an access code security does not give a clear direction for a successful termination of the apparent authority of a person who knows the access code because of a security breach. This uncertainty may affect the protection of the consumer against fraudulent payment losses.

Another aspect of the loss allocation rule that is controversial and which was discussed earlier in the other two jurisdictions, is the requirement that the access device must be

returned before notice of a potential misuse of the device can effectively terminate the authority of its user.<sup>128</sup>

In so far as a credit card is concerned, the CC Guidelines do not allocate losses based on misuse. Therefore, it is believed that the payment initiated by an authorised person though disapproved by the consumer, is treated as authorised when the card is not reported as lost or stolen. Accordingly, a consumer cannot terminate the apparent authority of the card user by giving notice of potential misuse to the issuer. Eventually, the issuer may qualify the protection the consumer against unauthorised payment by requiring the return of the card or closing of the account. In fact, the issuer may also insert a clause which allows it to allocate all the losses caused by the unauthorised use of the card to the consumer if he fails to return the card to the issuer without committing an offence against the Payment Systems Act 2003 since that duty does not contradict the EFT Guidelines.<sup>129</sup>

On the other hand, in the case of an EFT payment, Para 15 (3) of the EFT Guidelines allows the consumer to terminate the apparent authority of an authorised person by telling the issuer about debit card misuse. Eventually, this notice will limit the consumer's liability only to the losses incurred before the notification. Based on this rule, it is believed that the issuer cannot impose on the consumer a duty to return the additional debit card which is being misused before the consumer is protected against

---

<sup>128</sup> See above pages 78 85 and page 106-110.

<sup>129</sup> Section 57 read together with s. 26 (1) (c) and s. 71(1) of the Payment Systems Act 2003.

future losses. To impose that extra duty is an offence under s. 57 of the Payment Systems Act because it contradicts the EFT Guidelines.<sup>130</sup>

*(b) Apparent authority and the duty to examine the statement of account*

Generally, a consumer is not responsible for examining his statement of account and for reporting any recorded fraudulent payment to the issuer. However, if he comes to know about that payment, his failure to tell the issuer of the payment may constitute negligence and become a ground of allocating the losses to him. This rule is identical to the rule applicable to the cheque payment system in the United Kingdom as confirmed by the Malaysian Supreme Court in the case of the *United Asian Bank Bhd v Tai Soon Heng Construction Sdn Bhd*.<sup>131</sup>

The CC Guidelines' total silence as to the importance of checking the statement of account and the impact of a failure to do so on the consumer's liability for a fraudulent payment, indicates its rejection of this type of loss allocation rule in the credit card payment systems.

However, the contract terms of several credit agreements showed that the issuers chose to follow the remark made by the Privy Council in *Tai Hing Cotton Mill Ltd v Liu*

---

<sup>130</sup> Ibid.

<sup>131</sup> [1993] 1 MLJ 182, at 192.

*Chong Hing Bank Ltd*<sup>132</sup> where it emphasised that if the bank decided to impose on the consumer the duty to examine the statement of account, it can do so through its contract terms. Accordingly, if and when the duty is expressly incorporated in the contract, the consumer's failure to examine the statement of account constitutes a breach of contract, which therefore exposes him to the losses as provided in the contract.

In this respect, the decision in the case of *American Express Europe Ltd v Mervyn Leroy Fishback*<sup>133</sup> is useful to explain the effect of a contractual duty to examine the account statement. Mr Fishback disputed the amount of credit that he owed to the issuer. One of the issues considered by the court was whether Mr Fishback's failure to immediately inquire about the charges stated in his monthly statement meant that the amount was undisputed. The credit agreement entered into between the parties provided in clause 7(a) "If you have any queries about your monthly statement you must tell us immediately." In defining the term "immediately" the judge, considering the monthly statement that was received by the consumer, said "...it must mean as soon as reasonably possible and in any event before the issue of the following month's monthly statement."<sup>134</sup> Accordingly, it was held that the consumer was liable to pay the amount of the charges demanded by the issuer.<sup>135</sup>

---

<sup>132</sup> [1986] A.C. 80, at 103-107, *per* Lord Scarman on behalf of the law Lords.

<sup>133</sup> [1993] 335 MLJU 1 (Unreported Decision).

<sup>134</sup> *Ibid*, *per* Wan Adnan J, at 4.

<sup>135</sup> *Ibid*, at 5.

Although the case was not concerned with the consumer's liability for the payments debited to his account, the court's decision was useful in explaining the effect of having a contract term which would require the consumer to examine his account statement. The court held that the consumer must check the monthly statement when he received the statement and report any disputed payment, which may include any unauthorised payment found before the arrival of the next statement. By failing to do so, the consumer is assumed to have accepted the charges without dispute.

In the above case, the court did not consider the validity of the payment from the perspective of the agency rules. Had that issue been brought up by the consumer, the issuer might have shown that although the person who initiated the payment was not actually authorised by the consumer, the consumer's failure to check the statement of account and, to inform it of a fraudulent credit card payment, constituted a breach of contract which prevented the consumer from denying that payment. Eventually, the issuer may allocate the losses to the consumer based on the terms of their contract.

The EFT Guidelines differ from the CC Guidelines in this matter. In particular, Para 14 of the EFT Guidelines imposes on the consumer the duty to examine the account statement and to report any unauthorised payment that is recorded in the statement within 60 days from the date of the statement.

Despite a definite notification period, the EFT Guidelines do not explain the effect of the consumer's failure to perform that duty. A solution to this problem is similar to the one

suggested for the credit card payment, where the issuer may incorporate this duty in its contract with the consumer. Accordingly, when the issuer did not receive any information about an unauthorised payment because the consumer did not check his statement of account, which is a breach of a contractual duty, the issuer is justified in thinking that the payment was initiated by an authorised individual. Accordingly, the issuer may allocate the losses to the consumer as provided in the contract.

*(c) Apparent authority, duty of care and access code confidentiality*

Paragraph 15(1) (b) of the EFT Guidelines provides another circumstance when the debit card payment binds the consumer on the grounds of apparent authority. The provision states that the consumer has a duty to exercise reasonable care to keep the access code secret. Reading together this paragraph with Para 15 (2) which absolves the issuer from liability, it is clear that the EFT Guidelines allocate the losses to the consumer because his negligence *estopped* him from denying the EFT payment.<sup>136</sup>

Although the duty to exercise reasonable care rule is similar to the duty to exercise care in the cheque payment system, it is, however, not exactly identical because the exact replica of the rule would require the consumer to exercise reasonable care while making the EFT transaction but not in managing the access code security.<sup>137</sup>

---

<sup>136</sup> Vohrah, B. and Wu, M. A., *The Commercial Law of Malaysia*, at 388.

<sup>137</sup> See *Greenwood v Martins Bank Ltd* [1933] A.C. 51, 57, *London Joint Stock Bank v MacMillan and Arthur* [1918] A.C. 777, 835, and *Tai Hing Cotton Mill Ltd. V Liu Chong Hing Bank Ltd* 1986] AC 80,103-104. The same scope of consumer duty of care was held to apply in Malaysia in the cheque

An apparent authority arises when the consumer fails to exercise reasonable care in relation to the access code but not to the card because the definition of an access code in Para 3 does not include the card or any other tangible devices. Moreover, the consumer has to perform this duty in relation to an access code that is not associated with the card. This is to be understood by reading Para 15(1) (a), which requires the consumer to exercise a strict duty of confidentiality of “the access code of his card” together with Para 15 (1)(b). Since Para 15(1)(a) refers to an access code that is associated with the card, it is believed Para 15(1) (b) is referring to an access code that is used in a payment transaction that does not rely on the card. After all, this definition is more logical than subjecting the consumer to two contradictory standards of behaviour with regard to the same subject matter; one of reasonable care and the other strict. In fact, since one rule specifically refers to an access code that is associated with the card, while the other refers to an access code in general, this can be understood to mean that the rules are intended to regulate the allocation of fraudulent payment initiated with the use of a different access mode through different EFT technologies.

By defining an access code in Para 15 (1) (b) in such a way, the rule in this paragraph can be extended to require the consumer to exercise reasonable care in protecting the confidentiality of the password or PIN given by the issuer to the consumer to enable him to access the account via the internet or the m-payment systems. Nevertheless, this rule may only apply to an EFT payment made via the m-payment system as Para 4’s

---

payment system. See the decision in *United Asian Bank Bhd v Tai Soon Heng Construction Sdn Bhd* [1993] 1 MLJ 182. Compare to the rules in s. 12.12 and 12.5 of the United Kingdom Banking Code.



definition of an EFT system includes fund transfers performed through “telephonic instruments”. It is, however, not clear whether the rule is applicable to a payment initiated through internet payment systems.

Despite the potential application of the rule to the m-payment system, it is important to remember that the PIN used in such a system or the internet payment system is usually issued by the payment intermediary and not by the issuer. Unless the issuer itself provides the m-payment or internet payment facilities and issues the PIN, the access code in Para 15(1) (b) cannot be interpreted to refer to the PIN issued by the payment intermediary, even if the m-payment or the internet payment facilities falls within the scope of “telephonic instruments” because the EFT Guidelines only apply to a relationship between the issuer and the consumer.

Based on this discussion, it is believed that the issuer cannot allocate to the consumer the losses from the fraudulent payment made via the internet or the m-payment systems, even if the payment was initiated using a PIN that was obtained by the user as a result of the consumer’s negligence unless the PIN was issued by the issuer, like in the case of an internet banking facility.

In conclusion, it can be observed that the consumer’s failure to exercise care in relation to the protection of access code confidentiality prevents him from denying the validity of the relevant payment because that negligent conduct which enabled another person to obtain and use the code created an apparent authority in the user to initiate the EFT

payment. However, the rule only applies to the payment initiated through the conventional EFT systems but not through the internet or m-payment systems because of a limited definition of the EFT system in the EFT Guidelines. Moreover, even if the m-payment system is considered as an EFT system, the rule may be used by the issuer to allocate the losses caused by a fraudulent mobile payment if the issuer is the one who provided the services and issued the access code.

*(d) Apparent authority and strict duty to maintain access code confidentiality*

The fourth situation where a consumer is liable for unauthorised EFT payment on the grounds of apparent authority is specified by Para 15 (1) (a) of the EFT Guidelines. This provision states that a consumer is strictly prohibited from disclosing the PIN or the electronic device for accessing his account to any person either directly or indirectly.<sup>138</sup> It is strict because it is not qualified by terms such as “reasonable care” or “exercise care”. Moreover, the word “shall” also indicates that the duty is mandatory rather than directory, thus allowing the issuer to allocate the losses to the consumer if the unauthorised payment was facilitated by the consumer’s conduct.<sup>139</sup>

This rule in Para 15(1)(a) forbids the consumer from disclosing the code that is associated with the card. However, it does not cover the card details because as argued

---

<sup>138</sup> *Cheong Seok Leng v Public Prosecutor* [1988] 2 MLJ 481, at 489, *Muip Bin Tabib v Dato James Wong Wan and Hamid Bin Tuanku Surur v Francis Loke*, [1971] 1 MLJ 246, at 249.

<sup>139</sup> *State of UP v Babu Ram* AIR 1961 SC 751, at 765 *per* Subba Rao J.

elsewhere card details are not an access code under the EFT Guidelines.<sup>140</sup> Accordingly, when the consumer disclosed his card details directly or indirectly, and they were used by a fraudster to initiate an EFT payment via the internet or m-payment systems, the issuer may use this rule or may devise its own rules to allocate the losses.

Apart from an access code that is associated with the card, Para 15(1) (a) also requires the consumer to protect the confidentiality of the electronic devices used to effect the EFT payment. This part of the rule in Para 15 (1) (a) is even wider and covers any devices that the consumer uses to make the EFT payment, apart from the debit card. In fact, by describing the devices as a tool to “effect” the EFT payment, the device may include any instrument such as a computer or a telephone which is used to facilitate the communication between the consumer and the issuer’s system in order to commence the payment transaction.

The second part of the rule in Para 15(1) (a) is most probably intended to cover the EFT payment transaction that is made through a system where the payment can be initiated without using the card and its associated access code. Hence, the rule can be applied to the payment initiated via home or telephone banking facilities. However, it is not clear how the consumer is expected to protect the confidentiality of the computer or the telephone when he or she lives in shared accommodation.

---

<sup>140</sup> Chapter two at 60-61.

Apart from the above uncertainty, it is also not clear how the consumer can disclose the access code or the electronic devices indirectly.<sup>141</sup> By qualifying the consumer's duty in this way, the EFT Guidelines impose on the consumer a broad duty to protect his account against the risk of fraudulent payment. Such a broad duty may affect the protection of the consumer against unauthorised payment in an environment where the terminal at which the access code is used is exposed to others' view.

In addition, the access code by itself without the card is not useful in an EFTPOS transaction. This rule, therefore, suggests that even if the EFT transaction was effected with the use of a clone card and the consumer's access code, the consumer is liable for the losses if the access code was obtained by a fraudster as a result of the consumer's direct or indirect disclosure of the code. Similarly, it also suggests that if the card was obtained via involuntary transfer but the code was obtained by an indirect disclosure, the consumer is still responsible for the payment initiated by the fraudster.

The loss allocation rule in Para 15(1)(a) is very damaging to the consumer, compared to the duty to exercise care in Para 15(1) (b). In particular, the rule in Para 15(1)(a) gives the issuer an opportunity to allocate unauthorised transactions caused by almost anything, no matter how remote is the causation link between the losses and the

---

<sup>141</sup> In at least two cases the words "directly and indirectly" have been used side by side with the words "expressly and implicitly" to indicate a clear and straight forward action compare to not straight forward action or action to be implied from circumstances. See *Mohamad Ezam Mohd Nor & Ors v Inspector General Of Police* [2001] 2 MLJ 481, at 499; *Public Prosecutor v Dato' Balwant Singh (No 1)* [2002] 4 MLJ 427, at 442. In Pearsall, J., *The Oxford Concise Dictionary*, the terms "direct" was referred to as "in a direct" or "straight forward manner" while "indirect" can be understood to mean not straight forward, at 405,406, and 721.

consumer's action or inaction, so long as the access code or the electronic devices are known by others.<sup>142</sup>

In fact, reading this rule from the perspective of Para 14(4) of the EFT Guidelines which accept proof of the proper functioning of the access code, card and the security of the EFT system as conclusive evidence of the validity of an EFT payment, it is clear that the rule is very disadvantageous to the consumer.<sup>143</sup> In particular, a combined application of the rules in Para 14(4) and Para 15(1)(a) allows the issuer to assume that the person who initiated the payment by using the consumer's debit card and PIN was an authorised user.

It can be concluded that the consumer's failure to observe the duty to exercise reasonable care in keeping the access code confidential and also the duty to strictly avoid disclosing the access code and the electronic devices directly or indirectly, will make him liable for the whole EFT payment initiated by the fraudster because that payment is not unauthorised. However, it is not certain from the provision of Para 15(1)(a) and (b), whether the consumer may limit his losses in the above circumstances by giving notice of a breach of the access code security as provided in Para 15(3). Presumably, because the consumer's failure to observe the duties created an apparent authority in the person who initiated the EFT payment, the consumer's notice to inform

---

<sup>142</sup> Beale, H. G., *Chitty on Contracts*, Paras 26-029-26-040.

<sup>143</sup> See Chapter five discussing the use of a conclusive evidence clause in a contract between the consumer and the issuer at 281-284.

the issuer of the misuse of his debit card or the breach of access code security should be effective in limiting his losses to those that occurred before the notification.

The duty to exercise reasonable care in relation to the access code, the access device and the card details do not apply to the credit card payment systems. Accordingly, the issuer cannot allocate the losses from an unauthorised payment to the consumer on the grounds of negligence, except when the credit agreement imposed these duties on the consumer. Although incorporating the duty in the contract may amount for a violation of the CC Guidelines, which is an offence against the Payment Systems Act 2003, the validity of the particular term which imposed the duty to exercise care remains effective and binding on the consumer.

## **5 COMPARISON AND CONCLUSION**

A survey by the Bank for International Settlement, which showed an impressive incremental volume of credit card and debit transactions and in value, year by year, indicates the importance of the credit card, charge card and debit card in the consumer market.<sup>144</sup>

The result of the study is not surprising, considering the importance of electronic communication technologies in the commercial sectors. In this type of market the said

---

<sup>144</sup>Bank for International Settlement, Committee on Payment and Settlement Systems of the Group of Ten Countries, "Statistics on Payment and Settlement Systems in Selected Countries", March 2005, at <<http://www.bis.org/publ/cpss66.pdf>> 177-180. (Visited 6<sup>th</sup> September 2005).

payment facilities are advantageous to both parties, the consumer and the merchant, because they are portable, provide easy payment, and at the same time, they provide the merchant with a good marketing scheme.

However, despite the advantages, these payment facilities are also vulnerable to attack by irresponsible individuals who desire easy profits at the expense of others. Fraudulent payments made by such individuals usually leave the consumer, the issuer or the merchant with losses which may jeopardise the value that each of them can receive from using these payment facilities.

In view of that, loss allocation rules were formulated to prescribe the rights and liabilities of the consumer and the issuer in the case of fraudulent payment. Indeed, the analysis in this chapter have revealed that the loss allocation rules in all three jurisdictions incorporate a variation of the rules which govern the relationship of an agent and principal, whereby the consumer's liability for the particular payment is determined by evaluating the authority of the person who initiated the payment.

In the above discussion, various features of the loss allocation rules applicable in the Unites States, the United Kingdom and Malaysia were analysed and examined. Some of the rules are identical in all three jurisdictions, while some others are exclusive to a certain jurisdiction only. The following are numerous points which differentiate the level of consumer protection provided by the relevant loss allocation rules to the consumer.

## **A      Transfer of Mode of Access and the Authority to Initiate Payment**

All the regulations in the United States and the United Kingdom, except the Banking Code, pointed to the use of agency rules to determine the validity of credit card and EFT payments. However, the extent to which the rule is used to protect the consumer may differ, depending on the interpretation of the rule. For example, by transferring the card to another person, the consumer is considered to have authorised the recipient to use the card to initiate payment from the consumer's account. However, the rule can be a problem if the card cannot be used except with the PIN. Does transfer of the card give the recipient the authority to initiate a payment?

Strict interpretation of all the loss allocation rules in all three jurisdictions will bind the consumer to the payment initiated with the card although the PIN was obtained by an illegal means.

However, in the United States, the court's interpretation of s. 133 (a) of the TILA in the case of *Ognibene* made it clear that when the payment required a combined access mode, voluntary transfer of only one access mode did not give the person who initiated the disputed payment an authority to initiate a payment from the consumer's account.

It is not known whether the same approach will be applied in interpreting the loss allocation rules in Malaysia and the United Kingdom.



## **B Notification Rule and Termination of Authority to Initiate the Payment**

All the loss allocation regulations commonly use the notification rule to protect the consumer against unauthorised payment. The notice terminates the authority of the person who was once authorised to initiate the payment or of the person who never had an authority in the first place, like when the payment card was lost or stolen. By getting the notice, the issuer would know that the mandate issued by the particular person is an invalid mandate.

The notification rules may differ from one jurisdiction to the next and from one regulation to the other. However, the purpose is to terminate the issuer's belief that the person who tries to initiate the payment is an authorised individual.

In the United States, under the TILA loss allocation rules, the consumer may terminate the appearance of the credit card user's authority by giving notice of the events that may facilitate unauthorised credit card payment. This notice is effective, no matter how soon or late it is given; and the consumer is protected from the losses except, to the maximum of \$50. On the other hand, the EFTA notification rule differs greatly from the TILA. In fact, the EFTA rules describe the different time frames for notification, the different effect of the consumer's failure to notify and also the circumstances where the consumer's delay in notification will not affect his protection against the losses caused by fraudulent EFT payment. It provides the consumer with clearer Guidelines about his

duty to notify, the consequence of his failure to notify and the impact of an effective notification.

A notification rule identical to the TILA rule is used in the United Kingdom. Section 84(3) of the CCA and s. 12.12 of the Banking Code did not fix a time frame for notification just like the TILA. However, the Banking Code notification rule for the charge card and the debit card differ from the CCA rule since it allowed the issuer to fix the notification period in its contract terms. Since failure to comply with the contract terms is negligent by virtue of s. 12.11 of the Banking Code, the consumer is *estopped* from denying the validity of the disputed payment because his failure to give timely notice manifested to the issuer that the person who initiated the payment was authorised to do so.

In Malaysia, an attempt was made to fix the time frame for notification in the CC Guidelines. If the time for notification was made clearer and more specific, it would help the consumer in removing the appearance of authority of the credit card user. However, the rule failed to specify the notification period in clear and exact terms. Instead it described the period “as soon as reasonably practicable” after the consumer discovered the loss or theft of his credit card. This rule makes it harder for the consumer to make an *ex ante* determination of the steps that he has to take to protect himself against fraudulent payment losses. By leaving the consumer to figure out by himself the best time to give the necessary notice, the rule imposed on the consumer the burden

to decide the appropriate standard of behaviour which he has to exercise to prevent fraudulent payment, not from his own perspective but the issuer's.

A similar general notification period is provided by the rule in Para 15 (3) and Para 16 of the EFT Guidelines. In fact, both required the consumer to inform the issuer of the loss or theft of his debit card; or the misuse of the card; or the breach of the access code security without a delay. Since the word "delay" is very general and it is not linked to a reasonableness qualification, it is more difficult for the consumer to be able to foresee the situation when his notice can effectively terminate the apparent authority of a person to initiate the payment from the consumer's EFT account. Furthermore, it is also uncertain whether the consumer's notification of an unauthorised payment that is recorded in the statement of account may protect him against the losses that occur as a result of his failure to observe the duty to exercise reasonable care in the protection of access code confidentiality. A similar uncertainty is also created in relation to the strict duty to maintain confidentiality of the access code and the electronic access device.

### **C The Person to be Served with Notification**

Another important point in relation to the notice to terminate the authority of a person to use the access device and/or the access code to initiate payment from the consumer's account, is the designation of the party to whom the notice is to be served. Because of the complex structure of the relationship between all the parties involved in the credit card payment transaction, finding the party to whom the appearance of authority is

represented is not easy. As shown in the discussion, this problem affects the effectiveness of the termination of a person's authority to initiate payment from the consumer's account and may prevent the consumer from denying the validity of the disputed payment. This problem is faced by the consumer who holds a credit card account in the United States because the TILA leaves the determination of the third party to whom notice is to be given to the consumer.

The same problem, however, does not occur in debit card payment in the United States, nor in credit card, charge card and debit card payments in the United Kingdom and Malaysia. The notification rule in EFTA, the CCA, the Banking Code, and the CC and EFT Guidelines all clearly require notice to be given to the issuer.

#### **D      The Scope of the Notification Rule**

The notification rules in the different regulations also differ in their scope. The TILA and CC Guidelines require the consumer to inform the issuer of the loss or theft of the credit card while the CCA requires notification of the loss, theft or potential misuse of the credit card. On the other hand, Banking Code notification rules apply to the cases of loss or theft of a charge card or debit card or a breach of access code confidentiality. These notification rules are not applicable to cases where an unauthorised payment was initiated through any mode other than the card and /or the PIN. Accordingly, when payment was initiated through the use of the card details, the consumer cannot be made

liable on the grounds of an apparent authority even if he did not give the required notification.

The TILA notification rule, which is limited to the loss and theft of the card, created uncertainty as to whether the consumer is obliged to examine the statement of account and to report the unauthorised payment that is recorded there. This issue was settled by the decision in the *DBI* case.

The same controversy is, however, avoided by the EFTA and also by the Malaysian EFT Guidelines, which specifically require the consumer to examine the statement of account and to notify the issuer of any unauthorised payment which he discovered from that examination. However, the two differ as to the effect of the consumer's non-compliance with the rule. Under the EFTA rule, consumer liability will increase, depending on whether the losses involved a lost or a stolen card. The EFT Guidelines are, however, silent on this matter; leaving the issuer to choose the liability it wishes to allocate to the consumer for the consumer's failure to observe that duty.

## **E Negligence and Loss Allocation**

Apart from the notification rule, some of the loss allocation rules also rely on negligence as a ground for allocating the losses from the disputed payment to the consumer. This is to be found in the rule which imposes on the consumer a duty of care in relation to the protection of payment facilities from unauthorised use. For example, the United

Kingdom Banking Code requires the consumer to exercise care to protect the security of the debit card and/or the charge card, the access code, personal information and other details which allow the user to initiate the debit card or the charge card payment. In Malaysia, the EFT Guidelines require the consumer to exercise reasonable care only in keeping the access code secret.<sup>145</sup>

The rules are identical because both required proof of the consumer's negligence in failing to protect the security of the card and/or the PIN at the time of the transaction and also in the management of their security from unauthorised use.

Despite the similarity, the rule in the Banking Code is more specific and clearer than the EFT Guidelines. In particular, s.12.5 of the Code listed all the security measures which the consumer is expected to undertake to prevent unauthorised payment. The same details are missing from the EFT Guidelines. Paragraph 15(1) (b) of the EFT Guidelines only demand that the consumer should exercise care in relation to his access code, without specifying the actions to be taken to observe that duty.

## **F Strict Duty to Protect Access Code Confidentiality**

The duty of strict confidentiality is only prescribed by the Malaysian EFT Guidelines. Paragraph 15(1) (a) imposed on the consumer, albeit in vague and ambiguous terms, a

---

<sup>145</sup> Paragraph 15 (1) (b) of the EFT Guidelines reads "A customer shall not fail to take reasonable care to keep the access code secret."

strict duty not to “directly or indirectly”, disclose the debit card access code or the electronic means of accessing the account. This provision did not describe the acts to be undertaken or avoided but by a mere reference to the manner of the disclosure. The effect of the rule is that the consumer may be subjected to the losses if the issuer can prove that the consumer had disclosed the access code or electronic devices to another person.

A strict duty of confidentiality involving indirect disclosure of the access code or the electronic access devices in Para 15(1) (a) is disadvantageous to the consumer because indirect disclosure is a very broad description of a behaviour which may include disclosure of the PIN at the merchant counter when the consumer makes a payment. Accordingly, if the consumer indirectly discloses the PIN to other customers, and one of them later misuses the information, the consumer can be liable under Para 15(1)(a) of the EFT Guidelines, read together with Para 15 (2).

Apart from the above problem, the electronic devices used to effect an EFT payment may be inconspicuous particularly, in a family house or shared accommodation or even in an office where a telephone or computer are usually placed in an open space. Thus in that circumstances, is it difficult for the consumer to ensure that his transaction is not observe by others. In some situations, he may not be able to prevent the user of the device from accessing the record of the transaction. For instance, in the case of the internet transaction where the technology used usually allows cookie to capture data and

store them, it is hard for the consumer to know whether the information he entered into the system is being observed by others.

Therefore, to make the rule clearer, the term electronic devices should be specifically defined, so the consumer would know the type of transaction which will expose him to the potential liability if others indirectly observe him when he makes a transaction. Furthermore, the rule should also be amended to refer only to fraudulent behaviour of the consumer, similar to the one used in the CC Guidelines and also the TILA and the EFTA. The amendment is necessary because direct or indirect disclosure is too general a description of behaviour, which is difficult for the consumer to measure, hence, reducing the effectiveness of the rule in inducing the consumer to take action to prevent unauthorised payment.

Although Para 15(1)(a) of the EFT Guidelines' strict duty to maintain access code confidentiality overlaps Para 25 (1)(b)'s rule, discussed in section E on page 149 to 150, which requires the consumer to exercise reasonable care to protect the security of the access code, the first rule only apply to an action that amounts to a disclosure.<sup>146</sup> Moreover, the use of the conjunction "or" between Para 1(a) and 1 (b) shows that the issuer can allocate unauthorised payment losses to the consumer by relying on any of the two rules. Therefore, if the issuer can prove that the consumer had directly or indirectly

---

<sup>146</sup> Paragraph " 15(1) A customer shall not (a) directly or indirectly disclose to any person the access code of his card or any electronic device used to effect an electronic fund transfer; or (b) fail to take reasonable care to keep the access code secret."



disclosed the access code to another person, the losses are the consumer's. Alternatively, if the issuer does not have enough evidence of a disclosure but an unauthorised payment nonetheless occurs, the issuer may prove that the payment would not have happened if the consumers had done what an ordinary person would have to protect the access code confidentiality.

Looking from the said perspective, it can be concluded that the rules in Para (1) (a) and (b) of the EFT Guidelines protect the issuer from the losses caused by an unauthorised payment instead of protecting the consumer. This is not surprising considering that the Guidelines was issued by the BNM by virtue of its authority under the Banking and Financial Institutions Act 1989, a statute that regulate the business of banking and financial institutions.<sup>147</sup> Although the BNM authority to enforce these Guidelines has now being placed under the Payment Systems Act 2003, the same comment applies because the Act was passed to regulate the business of payment systems and not the consumer.<sup>148</sup>

---

<sup>147</sup> See the preamble to the Banking and Financial Institutions Act 1989 which states that it is an "[a]n Act to provide new laws for the licensing and regulation of institutions carrying on banking, finance company, merchant banking, discount house and money-broking businesses, for the regulation of institutions carrying on certain other financial businesses, and for matters incidental thereto or connected therewith".

<sup>148</sup> The preamble to the Act says, "[a]n Act to make provisions for the regulation and supervision of payment systems and payment instruments and for matters connected therewith."

## **CHAPTER FOUR                      LOSS ALLOCATION RULES: RECEIPT OF BENEFIT, FRAUD AND BURDEN OF PROOF**

### **PART I                      RECEIPT OF BENEFIT AND FRAUD**

#### **1                      INTRODUCTION**

The discussion in Chapter three showed that if the issuer cannot prove the presence of actual or apparent authority of the person who initiated the payment, it couldn't claim a repayment for the credit card or the EFT transaction from the consumer. However, that rule is not the only method of allocating fraudulent payment losses between the consumer and the issuer. Indeed, two of the electronic payment systems regulations discussed in this study, the Banking Code and the Malaysian EFT Guidelines, also incorporated a negligence-based loss allocation rule.

Moreover, in the United States, the TILA and the EFTA also distribute fraudulent payment losses based on the receipt of benefit rule.<sup>1</sup> In addition, the EFTA also allocate the losses by using the fraud-based rule. The said rule is also used in the United Kingdom Banking Code and the Malaysian CC Guidelines.<sup>2</sup>

---

<sup>1</sup> Section 103(o) of the TILA and s. 903(11) (A) of the EFTA.

<sup>2</sup> Section 903(11)(B), s. 12.12 of the Banking Code and Paras 13.2 and 13.3 of the CC Guidelines.

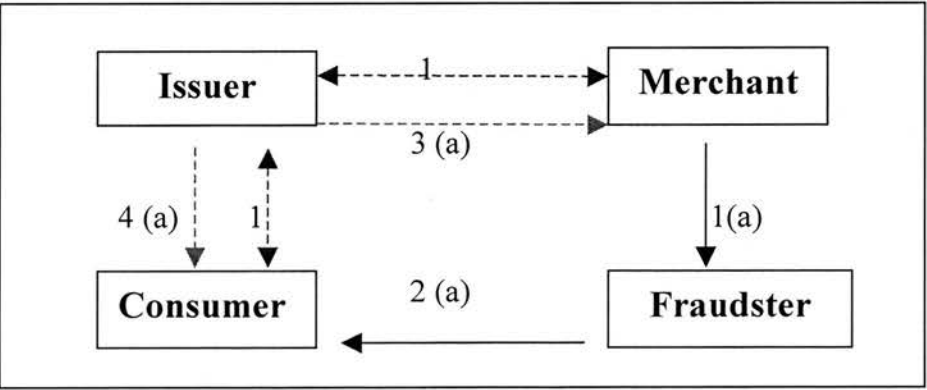
As Chapter three analysed the agency-based and negligence-based loss allocation rules, this chapter will examine the application of the receipt of benefit rule and the tort of deceit rule in the loss allocation process. Part 2 discusses the rule which allocates losses on proof of receipt of benefit by the consumer and Part 3 analyses the allocation of the losses when the consumer himself or a person with whom he cooperated acted fraudulently.

**2 LOSS ALLOCATION BASED ON RECEIPT OF BENEFIT**

**A Unjust Enrichment, Agency of Necessity and “No Profit from Fraud” Rule in the United States**

Before discussing in detail the rule which allowed the issuer to claim a repayment from the consumer for the benefit received from the unauthorised payment, Diagram 4.1 shows the transactional flow of the disputed payment.

Diagram 4.1 Payment for goods or services



In this diagram the issuer is not the one that sold goods or supplied services to the fraudster. Its function is to pay to the merchant the price of the goods or the services sold or supplied by the merchant to the purported authorised individual. In this arrangement, the consumer has a contractual relation with the issuer. (Step 1). Similarly, the merchant that supplied goods or services to the consumer also has a contractual relationship with the issuer, sometimes through the merchant acquirer.<sup>3</sup> (Step1). The transaction began when the fraudster contracted for the sale of goods or of supply of services with the merchant, who later on transferred the goods or the services to the fraudster. (Step 1 (a)). The fraudster then transferred the goods or the services to the consumer. (Step 2 (a)). The issuer paid the merchant as in steps 3 (a) and claimed a repayment from the consumer. (Step 4 (a)).

A problem occurs when the issuer cannot prove that the party who used the consumer's access devices or access code was authorised to initiate the payment. As a result, the issuer's act of paying the merchant for the goods or the services at the request of the fraudster falls under the category of unauthorised action of an agent that cannot bind the principal to the consumer.<sup>4</sup> Since the issuer can only debit the consumer's account with his mandate or the mandate of an authorised person, the payment cannot be debited to his account, be it an asset account in the case of an EFT payment or a credit account in

---

<sup>3</sup> See Smith, M. and Robertson, P., "Plastic Money", in Brindle, M. and Cox, R., *Law of Bank Payments*, Chp 4, at para 4-051. See *Suburban Nat'l Bank v. Transamerica Ins.*, 438 N.W. 2d 119 (Minn. Ct. App. 1989) which described the relationship.

<sup>4</sup> See Chapter One at 35-37.

the case of a credit card payment.<sup>5</sup> As a result, the issuer has to bear the losses since the payment is regarded as being made with its own funds.

However, in the United States, s.103 (o) of the TILA and s. 903(11) of the EFTA provides that a payment is not unauthorised if the consumer received benefit from it although the payment was made without his consent or authorisation.<sup>6</sup> Therefore, under the TILA and the EFTA, a payment initiated by an unauthorised person is not unauthorised if the consumer is proven to have received benefit from that payment.

The receipt of benefit rule affects the allocation of the fraudulent payment losses between the issuer and the merchant by changing the unauthorised status of the disputed payment to an authorised one. As a result, the consumer cannot claim the protection of the TILA or the EFTA against the losses caused by the disputed payment.

The TILA and the EFTA do not explain the basis for the receipt of benefit rule. A brief look at the rule suggests that it is based on agency by ratification.<sup>7</sup> However, agency by ratification requires proof of several conditions<sup>8</sup> including that the transaction was made on behalf of the consumer.<sup>9</sup> Since it is hardly the case that the fraudster made the unauthorised transaction on behalf of the consumer, receipt of benefit by the consumer cannot constitute ratification of the act of an unauthorised agent.

---

<sup>5</sup> See Chapter two for a discussion on the role of a payment mandate at 39-43.

<sup>6</sup> Section 103(o) of the TILA and s. 903(11)(A) of the EFTA.

<sup>7</sup> Section 98 of the Restatement (Second) of Agency 1958. See 2A *Corpus Juris Secundum* Agency § 71, and also 3 *Corpus Juris Secundum* Agency § 513. See *The Atlanta*, 82 F. Supp. 218 S.D. Ga. 1948).

<sup>8</sup> Section 84 -99 of the Restatement Second Agency.

<sup>9</sup> Section 98 comment c of the Restatement of Agency 1958.

From the nature of the disputed payment it is possible to argue that the benefit was conferred by the issuer as a result of a mistake caused by fraud. In that circumstance, it is suggested that the TILA's "receipt of benefit" rule, and surely, it should also apply to the EFTA, is based on restitution for unjust enrichment.<sup>10</sup> Unjust enrichment allows the issuer to claim restitution for the benefit unjustly received by a person at the issuer's expense.<sup>11</sup>

It should be noted that although the rule appears to be straight forward, applying it to credit card and EFT payment transactions is nonetheless complicated by the intricate web of the parties' contractual relationships, which involved a number of transfers of benefits between the parties. On the one hand, there is a transfer of benefit in the form of a money value between the issuer and the merchant. On the other hand, there is a transfer of benefit in the form of goods and/or services between the fraudster and the merchant. Similarly, there is also a transfer of goods and/or services from the fraudster to the consumer. In this scenario, it is difficult to identify the benefit conferred by the issuer as the benefit received by the consumer.

Generally, a claim in restitution for unjust enrichment is allowed if the recipient received the benefit directly from the claimant. Diagram 4.1 shows that the benefit received by the consumer came from the fraudster but not from the merchant or the issuer.

---

<sup>10</sup> Weistart, J. C., "Consumer Protection in the Credit Card Industry: Federal Legislative Controls", (1972), 70 *Mich. L. Rev.* 1475, at 1523-1525. (Hereafter Weistart, J., "Consumer Protection in the Credit Card Industry") Baron, R. G., *The Law of Restitution*, 6<sup>th</sup> Edn. (2002), 11-15, Sweet & Maxwell. (Hereafter, Baron, R. G., *The Law of Restitution*).

<sup>11</sup> Section 9 and s. 1 comments a, b, and c of the Restatement (First) of Restitution 1937, See Baron, R. G., *The Law of Restitution*, at 16-71.

Accordingly, the issuer cannot claim restitution for unjust enrichment against the consumer. Instead it has to lay an action against the fraudster for restitution.<sup>12</sup>

The problem of treating the benefit received by the consumer from the fraudster as the benefit received from the issuer may, however, be settled in the United States, by referring to s. 40 of the Restatement (First) of Restitution 1937 (the “Restatement of Restitution”) which allows the claimant to bypass the immediate recipient and go against the remote recipient if it was conferred upon the third party’s fraud.<sup>13</sup> Since benefit includes “services beneficial to or at the request of another” and the fraudster obtained the payment services by fraudulently representing himself as an authorised credit card or EFT system user, it is believed that the TILA’s and the EFTA’s receipt of benefit rule is based on s. 40 of the Restatement of Restitution.<sup>14</sup>

Before the issuer can rely on this solution, it has to prove that the consumer has knowledge of the benefit received from the fraudster.<sup>15</sup> Although the EFTA and the TILA are silent as to the nature of knowledge which the consumer must have s.10 (2) of the Restatement shows that knowledge can either be actual knowledge or constructive knowledge. So for instance, if the benefit was used for the consumer’s household and it was not obvious where it came from, the issuer probably cannot claim the value of the

---

<sup>12</sup> 42 *Corpus Juris Secundum* Implied Contracts § 29. See *Lazzarevich v. Lazzarevich*, 200 P.2d 49, 88 C.A.2d 708.

<sup>13</sup> Section 1 comment b of the Restatement (First) of Restitution 1937 defined “benefit” to include the performance of “services beneficial to or at the request of the other”. See *Lazzarevich v. Lazzarevich*, 88 Cal.App.2d 708, 200 P.2d 49 Cal.App. 2 Dist. 1948, at 716.

<sup>14</sup> See Weistart, J., “Consumer Protection in the Credit Card Industry: Federal Legislative Controls”.

<sup>15</sup> *Campbell v. Tennessee Val. Authority* 421 F.2d 293 C.A. Ala. 1969.

payment made to the merchant based on the “receipt of benefit” rule though it is possible to rely on agency of necessity.<sup>16</sup> But if the presence of the benefit is in such circumstances that the consumer should question its origin the consumer’s failure to enquire may amount to constructive knowledge<sup>17</sup> and therefore he would be liable to repay the issuer for the value of the service.<sup>18</sup>

The requirement of knowledge should be part of the TILA and the EFTA receipt of benefit rule since it is unfair to impose the losses on the consumer while he did not agree to receive the benefit in the first place and there was no opportunity to refuse.<sup>19</sup>

Another aspect of the “receipt of benefit” rule that is less clear is the measure of restitution which the issuer is entitled to claim. The wording of s. 103 (o) of the TILA and s. 903 (11) the EFTA which refer to unauthorised payment “from which the consumer [card holder] receives no benefit” indicates that when there is a receipt of benefit by the consumer, the payment is considered as authorised. As a result, the consumer may be made liable for the whole amount of the fraudulent payment losses, regardless of the actual amount of receipt. However, a claim for unjust enrichment is limited to the claimant’s expenses which had enriched the recipient. Accordingly,

---

<sup>16</sup> See Weistart, J., “Consumer Protection in the Credit Card Industry: Federal Legislative Controls”, at 1524-1525. See s. 22 of the Restatement (Second) of Agency 1958 comment c and cross-reference to s. 113 of the Restatement (First) of Restitution 1937.

<sup>17</sup> See s. 10 (2) and comment d of the Restatement (First) of Restitution 1937. Also Comment a to s. 9 of the Restatement (Third) of Restitution And Unjust Enrichment (Tentative Drafts)

<sup>18</sup> The acceptance by the consumer of the service may fall under the category of unjust enrichment by “free acceptance” as explained by Baron, R.G., *The Law of Restitution*, at 28-31, except that a claim based on indirect enrichment is not recognised in English law and Scots law.

<sup>19</sup> Comment b to s. 40 of the Restatement (First) of Restitution 1937. See *Lawson v. O’Kelley*, 81 Ga.App. 883, 60 S.E.2d 380 (1950).



despite the generality of the rule, the measure of the claim should be limited to the value of the benefit received by the consumer on the basis of *quantum meruit*.<sup>20</sup>

The effect of the consumer's "receipt of benefit" to the allocation of the losses from unauthorised credit card payment in the United States was explained in many cases including the case of *Mastercard, Consumer Credit Div. of First Wisconsin Nat'l Bank of Milwaukee v. Town of Newport*,<sup>21</sup> and *Blaisdell Lumber Co., Inc. v. Horton*.<sup>22</sup> In these cases, the court stated that the unauthorised credit card use under s.103 (o) of the TILA refers to the use of the card by a person other than the consumer; when the user did not possess actual or apparent authority; and the consumer did not receive benefit from that use.

Finally, the receipt of benefit rule as used in the TILA and the EFTA also lacks clear direction as to the nature of the benefit which they cover. The question is, does the benefit include any type of benefit received by the consumer even if it did not come directly from the unauthorised payment?

The receipt of benefit rule was applied in the case of *Citibank (South Dakota), N.A. v. Gifelman*<sup>23</sup> involving a credit card payment initiated using a secondary card. The undisputed facts of the case showed that the consumer received a \$25.00 monthly

---

<sup>20</sup> Section 9 comment b and c of the Restatement (Third) of Restitution And Unjust Enrichment (Tentative Drafts). See Section 40 comment f of the Restatement of Restitution and *Telespectrum Worldwide, Inc. v. Grace Marie Enterprises, Inc.* Unreported in F.Supp.2d, 2001 WL 322584 E.D.Pa.,2001

<sup>21</sup> 133 Wis. 2d 328, 396 N.W.2d 345, 347 (Ct.App.1986).

<sup>22</sup> 242 N.J.Super 98, 104, 575 A.2d 1386, 1389 N.J.Super.A.D.,1990.

<sup>23</sup> 63 Conn.App. 188, 773 A.2d 993 Conn.App.,2001.

payment from the person to whom a secondary card was issued with the consumer's consent. A dispute arose as to whether the issuer was entitled to claim the charges made using the secondary card. The appellate court held the consumer responsible for the charges because he had authorised the card usage and also because he had received monetary benefit from the issuance of the relevant card in the form of a monthly fee payment. Therefore, with the proof of authority and also receipt of benefit the disputed charges fell outside the scope of unauthorised payment under s. 103 of the TILA.<sup>24</sup>

It appears that the court in the Citibank's case extended the scope of the "receipt of benefit" rule to cover the benefit received not only from the disputed payment but to the money received by the account holder as a consideration for applying and giving the supplementary card to another person.

If the language of s. 103 (o) of the TILA is analysed, it can be observed that the scope of the "benefit" is restricted by the description of unauthorised use of the credit card. Therefore, when the rule described unauthorised use of the credit card as the use "from which the card holder receives no benefit", the word "from" indicated that the "unauthorized use" of the card should be the source or the origin of the benefits received by the consumer.<sup>25</sup> Accordingly, the benefit received by the consumer in *Citibank (South Dakota), N.A. v. Gifelman*<sup>26</sup> cannot make him liable for the series of payments made with the use of the secondary credit card since the monthly payment was received

---

<sup>24</sup> Ibid, at 194.

<sup>25</sup> Pearsall, J., *The Concise Oxford Dictionary*, at 568.

<sup>26</sup> 63 Conn.App. 188, 773 A.2d 993 Conn.App.,2001.

in reciprocity for the giving of authority to the card holder to use the card. Even if the card was used by an unauthorised individual, that monthly payment did not originate from the “unauthorized use” of the credit card. Instead, the reason for finding the consumer responsible for the charges should be the authorised card usage.

The above argument should also apply to the receipt of benefit rule in s. 909 (11) (A) of the EFTA because the definition of “unauthorized electronic funds transfer” also covers the EFT transfer “from which the consumer receives no benefit”. From this phrase it appears that the benefit must come from the disputed EFT payment before the consumer can be liable for the disputed payment.

Apart from the restitution for unjust enrichment under s.40 of the Restatement of Restitution, the issuer may also claim restitution for the payment it has made to the merchant when the person who used the credit card or the debit card is a person who the consumer is bound by statutory or common law duty to support.<sup>27</sup> To claim on this ground, the issuer must show that the things supplied were necessities<sup>28</sup> and the defendant had failed to supply them to the recipient at the time the transaction took place.<sup>29</sup>

---

<sup>27</sup> Section 133 comment a of the Restatement (First) of Restitution 1937. See the Zitter, J. M., “Necessity, in Action against Husband for Necessaries Furnished Wife, of Proving Husband's Failure to Provide Necessities” (2006) 19 *A.L.R.* 4th 432, originally published 1983; Cross, M. L., “Husband's Liability to Third Person for Necessaries Furnished to Wife Separated from Him” (2006) 60 *A.L.R.*2d 7, originally published 1958; *Williston: A Treatise on Contracts*, Chp 9 Capacity of Parties – Infants, §9-24.

<sup>28</sup> See the definition of necessity in s. 113 comment d of the Restatement (First) of Restitution 1937. See also *Williston: A Treatise on Contracts*, §11:9.

<sup>29</sup> *Wanamaker v. Ulizio*, 102 N.J.L. 166, 130 A. 555 (E. & A.(1925)).

Accordingly, when the credit card or the EFT payment was initiated by the consumer's wife or the consumer's minor child, the payment is not unauthorised under the TILA and the EFTA loss allocation rules if the payment was for necessities.<sup>30</sup>

Finally, the third possible basis for the TILA and the EFTA receipt of benefit rules is the principle which says that that "... a person, though innocent, cannot avail himself of an advantage obtained by the fraud of another unless there is some consideration moving from himself".<sup>31</sup> According to this rule, the issuer may claim the benefit received by the consumer if he is not a bona fide purchaser for value without notice i.e., he purchased the benefit with notice, actual or constructive, of the defect in the seller's title, did not pay valuable consideration, and acted in bad faith.<sup>32</sup> To succeed in a claim on this ground, the issuer has to prove any of these three elements to negate the consumer's good faith.

From this discussion it is clear that a credit card or an EFT payment is not considered as an unauthorised payment under the TILA and the EFTA, if the consumer received

---

<sup>30</sup> The necessities of a child and a wife is different where the latter's scope of necessity is wider than the former. See Williston: *A Treatise on Contracts*, §11:9 and §9:19. The issuer's claim in restitution on ground of agency of necessity is not similar to a claim on the ground of the apparent authority of the wife to represent the husband to purchase household supplies. See s. 22 comment b and s. 141 comment c of the Restatement (Second) Agency 1958. See *Saks & Co. v. Bennett*, 12 N.J.Super. 316, 79 A.2d 479, 480 (1951); *Sullivan v. Ski Liberty Operating Corp.* 1999 WL 715183 Pa.Com.Pl. (1999) and *Medical Business Associates, Inc. v. Steiner*, 183 A.D.2d 86, 588 N.Y.S.2d 890 (2d Dep't 1992) and *Accounts Management, Inc. v. Litchfield*, 1998 SD 24, 576 N.W.2d 233 (S.D. 1998).

<sup>31</sup> *Atlantic Cotton Mills v. Indian Orchard Mills*, 147 Mass. 268, 17 N.E. 496 Mass. 1888, at 273. See also *Einar Glaser v. Dwight Holdorf* 56 Wash. 2d 204, 352 P.2d 212 (1960).

<sup>32</sup> *Morehead v. Harris*, 262 N.C. 330, 338, 137 S.E.2d 174, 182 (1964).

benefit from the disputed payment. This rule justifies the issuer's claim for a repayment on the principle of restitution and not on the mandate rule.<sup>33</sup>

It can be concluded that although there are potentially three bases for the rule, it is believed that the receipt of benefit rule found its root in the law of restitution for unjust enrichment under s. 40 of the Restatement of Restitution.

## **B Unjust Enrichment, Agency of Necessity and “No Profit from Fraud” Rule in the United Kingdom and Malaysia**

Compared to the TILA and the EFTA, which specifically allocate losses based on restitution for unjust enrichment for the benefit received by the consumer at the issuer's expenses, neither the United Kingdom loss allocation scheme nor the Malaysian scheme address liability based on receipt of benefit.

Apparently, it is possible for the issuer to insert into the credit agreement a term that provides that unauthorised credit card payment is to be allocated to the consumer if he received benefit from that payment. However, in so far as the credit card is concerned, s. 173 (1) and (2) of the CCA provides that the credit agreement cannot contradict the CCA loss allocation rules. Indeed subsection (2) shows that contradiction occurs when the contract terms stipulate different duties and liabilities for the consumer in the

---

<sup>33</sup> See Weistart, J., “Consumer Protection in the Credit Card Industry: Federal Legislative Controls”, at 1525.

circumstances which are already described by the CCA namely, loss or theft of the credit card, unauthorised payment in a distance transaction, or authorised use of the card.<sup>34</sup> Accordingly, when a consumer receives benefit from a unauthorised payment that occurs as a result of loss or theft of the credit card, or fraudulent payment in a distance contract, the issuer cannot impose on the consumer different loss allocation rules. Therefore, it is believed that in the case of a credit card payment, the issuer cannot contractually allocate losses from a fraudulent credit card payment based on the receipt of benefit rule since that contractual loss allocation contradicts the CCA.

However, the position may differ when the payment is made using the EFT system. The Banking Code does not have a provision similar to s. 173 of the CCA. Therefore, the issuer is not technically prohibited from allocating the fraudulent payment losses to the consumer if it can prove the consumer's receipt of benefit from the fraudulent payment. In fact, according to s.12.11, the issuer may contractually impose other contract terms on the consumer whereby the consumer's breach of that term eventually constitutes negligence that allows the issuer to allocate the losses to the consumer. Therefore, the issuer may provide in its contract that the consumer should not receive benefit from the disputed payment otherwise the payment is binding on him.

Apart from the contractual loss allocation, the Banking Code did not stipulate that its loss allocation rules are the only rules to be applied in a dispute involving EFT or charge card payments. The lack of restriction on the application of other loss allocation rules in

---

<sup>34</sup> Section 84 (1),(2) and (3A) of the CCA.

the Banking Code may give the issuer the opportunity to rely on a claim for restitution for unjust enrichment.

Similarly, the Malaysian CC and EFT Guidelines also do not forbid the issuer from using other loss allocation rules in allocating the losses from unauthorised credit card or EFT payments. Therefore, the issuer may specify in the credit or bank account agreement that a consumer should be responsible for an unauthorised payment if he received benefit from that payment.

Even if the contract terms did not contain the receipt of benefits rule, the Payment Systems Act 2003, which prescribed the penalty for failure to comply with the Credit Card and EFT Guidelines did not exclude any other legal remedy or equitable relief. This silence may be used as a basis to argue that the issuer may claim restitution for unjust enrichment for the benefit received by the consumer from the fraudulent payment.

Despite the potential of applying the law governing restitution for unjust enrichment to settle the allocation of fraudulent payment losses between the consumer and the issuer, such an approach is impossible because in Malaysia and the United Kingdom, a restitutionary claim for unjust enrichment can only be instituted against the defendant

who received the benefit at the issuer's expenses, i.e., an immediate recipient and not a remote recipient.<sup>35</sup>

Accordingly, in the United Kingdom, the issuer may claim restitution against the merchant for the latter's unjust enrichment since the payment was made by the issuer under a mistake of fact caused by the fraud of the third party.<sup>36</sup> The consumer is, however, free from liability because under English law, the claimant cannot leapfrog the first defendant and claim against the subsequent party who received the benefit because the remote recipient did not receive the benefit at the expense of the claimant.<sup>37</sup>

This rule was applied in the case of *R.E. Jones Ltd. v. Waring & Gillow Ltd.*<sup>38</sup> where the plaintiff who paid a certain sum of money to the defendant claimed a repayment of that sum because it was made under a mistake of fact caused by the fraud of a third. The court found for the plaintiff. Similarly, in *Barclays Bank Ltd v W. J. Simms Son and Cooke (Southern) Ltd.*<sup>39</sup> the bank succeeded in its claim for the payment received by the defendant when the payment was made because of a mistake of fact.<sup>40</sup>

---

<sup>35</sup> See for example the English case of *R.E. Jones Ltd. v. Waring & Gillow Ltd* [1926] A.C. 670 and *Barclays Bank Ltd v W. J. Simms Son and Cooke (Southern) Ltd* [1980] 1 QB 677. See also s. 71 of the Contracts Act 1950.

<sup>36</sup> Baron R. G., *The Law of Restitution*, at 192, 183-186. See the position in Scotland in Whitty, N. R., *Indirect Enrichment in Scots Law*, 1994 JR 200, at 252 – 267. (Hereafter Whitty, N. R., *Indirect Enrichment in Scots Law*).

<sup>37</sup> Birks, P., "At the Expense of the Claimant": Direct and Indirect Enrichment in English Law", in D. Johnston and R. Zimmermann (Eds), *Unjustified Enrichment: Key Issues in Comparative Perspective*, (2002), at 504-505, Cambridge University Press.

<sup>38</sup> [1926] A.C. 670.

<sup>39</sup> [1980] 1 QB 677. Birks, P., "At the Expense of the Claimant": Direct and Indirect Enrichment in English Law", at 504 -505

<sup>40</sup> [1980] 1 QB 677, at 695, and 699, *per* Goff J.



A similar rule applies in Malaysia. In *Chong Thian Fook V. Sarawak Shell. Berhad & 8 Ors*,<sup>41</sup> the court stated that a person who had conferred benefit upon another person may make a claim for unjust enrichment against the other person if the other person was enriched by that benefit. However, s. 71 of the Contracts Act 1950, which codified the common law rule of unjust enrichment, has specified four ingredients essential to a claim based on unjust enrichment namely:

- (1) the act done by the plaintiff must be lawful;
- (2) it was done for another person or individual;
- (3) it was not done gratuitously; and
- (4) it conferred benefit upon the other party.

From the above provision, the fourth element made it clear that in Malaysia, a claim based on unjust enrichment can only be made against the immediate recipient of the benefit and not against a remote recipient.

The above provision was applied in the case of *Jone Theseira v Eileen Tan Ee Lian & Anor*<sup>42</sup> where the plaintiff claimed a repayment from the defendant for the payment he had made to a hospital for the treatment given to the defendant's daughter. The court held that the payment, which was a lawful act, was made for the benefit of the defendant, the mother. The benefit was in the form of a postponement in the repayment of the money owed to the plaintiff until the defendant received her insurance claim.

---

<sup>41</sup> [2004] 7 MLJ 53, 90-92.

<sup>42</sup> [2002] 4 MLJ 629, at 636.

Moreover, the plaintiff did not intend to make a gratuitous payment but with the hope of getting a repayment from the defendant. Accordingly, it was held that the payment fell within the scope of a claim for unjust enrichment under s. 71 of the Contracts Act 1950.

Based on these authorities, it is clear that an issuer of a credit card, charge card or EFT payment facilities cannot claim restitution from the consumer for unjust enrichment even if the latter had received benefit from unauthorised payment through the fraudster.

Nevertheless, if the person who used the card without authority is a minor, or mentally ill or drunk, to whom the consumer owes a common law duty to take care, the issuer may claim restitution if he can prove that the goods and/or services were for the card user's necessities.<sup>43</sup> However, in the United Kingdom, the issuer cannot institute this claim if the disputed payment was made by the consumer's wife because the wife is not considered an agent of necessity by virtue of s. 41 of the Matrimonial Proceedings and Property Act 1970.

In Malaysia a claim based on agency of necessity may be instituted by the issuer against the consumer by virtue of s. 69 of the Contract Acts 1950 if the payment was initiated by a person who the consumer is legally bound to support.<sup>44</sup> This type of claim may be

---

<sup>43</sup> Beale, H. G., *Chitty on Contracts*, paras 8-002-8-074, 8-080 and 29-135.

<sup>44</sup> *Government Of Malaysia v Gurcharan Singh & Ors* [1971] 1 MLJ 211, 213-214.

made by the issuer against a consumer for an unauthorised purchase made by his wife or his children, or against a person is responsible for the consumer's child.<sup>45</sup>

Another alternative loss allocation rule for the issuer in the United Kingdom is to apply the "no profit from fraud" rule and claim restitution from the consumer for the benefit received by the latter through the fraudster, where the benefit comes from the fraudulent payment involving the consumer's credit card, charge card or debit card.<sup>46</sup> However, to succeed on this ground of claim, the issuer must show that the consumer did not give a valuable consideration to the fraudster and had acted *mala fide*.<sup>47</sup>

For example in the English case of *Re McCallum*,<sup>48</sup> the case involve the deed of conveyance of a property executed by the deceased in favour of her daughter but kept secret until after her death. The father who had continued in possession of the house died without knowing about the deed. The question was whether the daughter can bring an action to recover the house from the defendant who took possession of the house after the father passed away. On appeal by the defendant, the Court of Appeal held that the daughter was not a privy to the fraud. Accordingly, she cannot be barred from bringing the action to recover possession of the house.

---

<sup>45</sup> *Koh Yen Bee v American International Assurance Co Ltd* [2000] 7 MLJ 278.

<sup>46</sup> Gloag, W. M., *Introduction to the Law of Scotland*, 11<sup>th</sup> Edn (2001), 164, Whitty, N. R., *Indirect Enrichment in Scots Law*, especially at 257-258 and 266. See English authority in *Re McCallum* [1901] 1 Ch. 143, at 156, *per* Rigby L.J., quoted the principle as formulated in *Scholefield v. Templer* (1859) 28 Ch. 452 and the Scots authority in *M. & I. Instrument Engineers Ltd. v. Varsada* 1991 S.L.T. 106 which also referred to *Clydesdale Bank v. Paul* (1877) 4 R. 626, at 628-629 *per* Lord Shand L.J.

<sup>47</sup> Whitty, N. R., *Indirect Enrichment in Scots Law*, at 256-257

<sup>48</sup> [1901] 1 Ch. 143.

The same principle was held to apply in the case of *M & I Instrument v Varsada*. In this case the pursuer claimed restitution against the third party who received the profit of fraud committed by another individual against the company. Evidence showed that a large sum of the defrauded amount was used to purchase a property which title is registered in the name of the defender. The counsel for the defender argued that the general rule of law, which says that a third party is not to be permitted to profit from the fraud of another, does not apply to the case of money and negotiable instruments.<sup>49</sup> Lord Milligan rejected the argument and confirmed that this rule cannot apply to money only if the vindication of the profit, received by a third party bona fide, will be an impediment to commerce.<sup>50</sup>

The *M & I Instrument's* case confirmed the rule that if the consumer received benefit from the unauthorised payment, he cannot keep the profits unless he is bona fide and pays consideration for the profit. Even if the subject matter of the issuer's claim is the money, which the consumer received from the fraudster after a fraudulent withdrawal, the issuer may claim restitution by applying the "no profit from fraud rule" unless restitution will affect commerce.

Again, the issuer in Malaysia may also use the same rule. The fact that Malaysian laws are based on the common law rules of England unless other rules are enforced means

---

<sup>49</sup> *M. & I. Instrument Engineers Ltd. v. Varsada* 1991 S.L.T. 106, at 109-110.

<sup>50</sup> *Ibid*, 109.

that the issuer may institute a claim for restitution based on the “no profit from fraud” rule.<sup>51</sup>

However, it is not clear how far the agency of necessity rule or the “no profit from fraud” rule can be used by the issuer to allocate the fraudulent payment losses to the consumer since no records of the Mediation Bureau is available for reference.

In the United Kingdom, the Ombudsman’s decisions indicate that neither the rules of agency of necessity nor the “no profit from fraud” rule were raised by the issuer against the consumer.<sup>52</sup> Similarly, the Ombudsman also did not address the possibility of applying these two grounds of claiming restitution in its decision though there was an opportunity to do so.<sup>53</sup> The Ombudsman’s indifferent attitude to these two rules implies that the issuer and the Ombudsman treat the loss allocation rules in the CCA and the Banking Code as conclusive allocation schemes without the needs to look further.

### **3 LOSS ALLOCATION AND CONSUMER FRAUD**

Another loss allocation rule incorporated in the credit card and EFT regulations in the EFTA, the United Kingdom Banking Code and the Malaysian CC Guidelines is the rule

---

<sup>51</sup> Section 3(1) of the Malaysian Civil Law Act 1957.

<sup>52</sup> See the Ombudsman decisions in its monthly newsletter at <<http://www.financial-ombudsman.org.uk/publications/ombudsman.htm>> (Visited 1<sup>st</sup> January 2006).

<sup>53</sup> See the Ombudsman decision no 46/2 a <[http://www.financial-ombudsman.org.uk/publications/ombudsman-news/46/46\\_plastic\\_cards.htm](http://www.financial-ombudsman.org.uk/publications/ombudsman-news/46/46_plastic_cards.htm)> (Visited 1<sup>st</sup> January 2006).

that allows the issuer to claim restitution for wrong.<sup>54</sup> In order to succeed in its claim, the issuer must prove that the consumer had, either by himself or in joint effort with another, acted fraudulently.

Section 903(11) (B) of the EFTA specifically provides that any unauthorised EFT payment initiated with fraudulent intent, either by the consumer himself or by another person with whom the consumer acted in concert is not an unauthorised payment. If the issuer can prove that the consumer is party to the fraud, it can claim restitution against the consumer.<sup>55</sup>

The specific reference to the intention to commit fraud in the EFTA was probably inserted with the intention to prevent an inconsistent application of the rule in different state jurisdictions because of the different requirement of proof of fraud in different American states. In some states, proof of fraud must include proof of intention to deceive<sup>56</sup> while in some other states, an action on fraud requires proof that the person who made the false representation intended the false representation to be relied on and acted upon by the person to whom it is represented to that person's detriment.<sup>57</sup>

---

<sup>54</sup> Birks, P and Chambers, R., "The Restitution Research Resource 1994" (1994) *R.L.R.* Supp. at vi-vii; Jackman, I. M., "Restitution for Wrongs", 48 *Cambridge L.J.* 302 (1989), and Mather, H, "Restitution as a Remedy for Breach of Contract: The Case of The Partially Performing Seller", (1982) 92 *Yale L.J.* 14, at 42

<sup>55</sup> *Klein v. Equitable Life Assurance Soc.* (1984), 17 Ohio App.3d 50, 17 OBR 105, 477 N.E.2d 1190.

<sup>56</sup> *South Branch Lumber Co. v. Ott*, 142 U.S. 622, 12 S. Ct. 318, 35 L. Ed. 1136 (1892); *Froelich v. Erickson*, 96 F. Supp. 2d 507 (D. Md. 2000). See 37 *Am. Jur.* 2d, Fraud and Deceit ss. 107 and 113.

<sup>57</sup> *In re Chavin*, 150 F.3d 726 (7th Cir. 1998); *In re Tallant*, 207 B.R. 923 (Bankr. E.D. Cal. 1997), *Fletcher v. Edwards*, 26 S.W.3d 66 (Tex. App. Waco 2000); *City of Atascadero v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*, 68 Cal. App. 4th 445, 80 Cal. Rptr. 2d 329 (1st Dist. 1998), *Damon v. Sun Co., Inc.*, 87 F.3d 1467 (1st Cir. 1996); *Foiles v. Midwest Street Rod Ass'n of Omaha, Inc.*, 254 Neb. 552, 578 N.W.2d 418 (1998). See 37 *Am. Jur.* 2d, Fraud and Deceit, ss 107 and 113.

Therefore, the requirement of fraudulent intent in the EFTA is necessary to promote uniform application of the EFTA loss allocation rules in all the states.

The loss allocation rule in the United Kingdom Banking Code and the Malaysian CC Guidelines, which also allocate losses based on the consumer's fraud, differ from the EFTA's rule since they do not specifically and expressly require that the fraud must have been committed with "fraudulent intent".<sup>58</sup> This is because in these two jurisdictions, the plaintiff need not prove intention to defraud but that the defendant made the representation hoping that it would be acted upon by the party to whom it was made.<sup>59</sup>

Despite the differences, the effect of the fraud rule is identical in all three jurisdictions since it excludes the consumer from the protection of the respective regulations against unauthorised payment.

It should be noted that although it is hard to find a case that explains the scope of fraud used in the EFTA, the Banking Code and the EFT Guidelines loss allocation schemes, authorities that deal with the general rule of fraud are plenty and helpful in setting the scope of the rule.

---

<sup>58</sup> Section 12.11 and 12.12 of the Banking Code, and Para 13.2 and 13.3 of the CC Guidelines.

<sup>59</sup> *Stafford Winfield Cook & Partners Ltd v Winfield* [1981] 1 WLR 458, at 466, *per* Megarry VC and *Jaffray & Ors v. Society of Lloyd's*, [2002] EWCA Civ 1101 (C.A.); *Bank Bumiputra Malaysia Bhd V Yeoh Ho Huat* [1979] 1 MLJ 30, and *Magnum Finance Bhd v Tan Ah Poi & Anor* [1996] 538 MLJU 1.

Generally, in all three jurisdictions, fraud by representation is defined, based on the remark made by Lord Herschell's in the case of *Derry v. Peek*<sup>60</sup> namely, "fraud is proved when it is shown that a false representation has been made (1) knowingly, or (2) without belief in its truth, or (3) recklessly, careless whether it be true or false."<sup>61</sup>

Therefore, for the issuer to prove fraud, it must be able to show that the representation made by the consumer was made while the consumer knows that it was false or he does not care whether it was true or false. In the electronic payment system via a credit card or EFT system, the fact which constitutes fraudulent false representation is the consumer's false promise to pay for the purchase he made. This promise is made each time the consumer, or a person with whom he is cooperating, uses the access device and/or code but not at the time when the consumer entered into the contract for the payment facilities.<sup>62</sup>

Accordingly, when the consumer himself used the payment card or the access code or allowed another to use it without the intention of paying the issuer for that usage, he had

---

<sup>60</sup> (1889) 14 App Cas 337, [1886-90] All ER Rep 1.

<sup>61</sup> *Shwab v. Walters* 147 Tenn. 638, 644, 251 S.W. 42, 44 (1922), *Neurosurgery And Spine Surgery, S.C v Mary Goldman* 339 Ill. App. 3d 177; 790 N.E.2d 925 (2003); *Bank Bumiputra Malaysia Bhd v Yeoh Ho Huat* [1979] 1 MLJ 30, at 36, *Magnum Finance Bhd v Tan Ah Poi & Anor* [1996] 538 MLJU 1; *Stafford Winfield Cook & Partners Ltd v Winfield* [1980] 3 All ER 759 at p 766 and *Jaffray & Ors v. Society of Lloyd's* [2002] EWCA Civ 1101 (C.A.)

<sup>62</sup> This view is in line with the view in cases involving nondischargeable credit card debt due to fraud in the United States under the Section 523 of the Bankruptcy Code 11 U.S.C.A. See Black, E. L., "Credit card debt as nondischargeable under Bankruptcy Code provision concerning nondischargeability of individual debt obtained through false pretenses, false representation, or actual fraud, other than statement respecting debtor's or insider's financial condition" (2006) 158 *A.L.R. Fed.* 189, originally published 1999. See the position in the United Kingdom on the issue of discharge of bankruptcy and fraud in s. 281 (3) of the Insolvency Act 1986 and the case of *Mander v Evans* [2001] 3 All E.R. 811 (Ch D); and in Malaysian in s. 33 (1) and (6)(k) of the Malaysian Bankruptcy Act 1967.



made a false representation of fact which induced the issuer to advance the credit and pay the merchant for the purchase.<sup>63</sup> Therefore, the consumer should be liable for the losses because it is said, “no man shall be permitted to take the chance of committing fraud, without running any risk of losing by the event, when it is detected”.<sup>64</sup>

The fraud-based loss allocation rule is neither used as a basis for allocating fraudulent credit card payment in the CCA and the TILA, nor for allocating fraudulent EFT payment in the Malaysian EFT Guidelines. Although the TILA states that it is an offence for a person to use or partake in interstate or foreign commerce which involves a “counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained credit card”, the provision does not refer to a situation where the consumer used his legally obtained card and/ or access code or allowed another to use it without any intention of paying for the charges.<sup>65</sup> In the other two regulations, no fraud rule can be found at all.

It is possible that the drafters of the TILA left the fraud-based loss allocation rule because TILA already has the receipt of benefit rule, which is sufficient to catch the consumer who allowed another person to use the access device fraudulently and at the same time, received benefit from that usage. However, the most possible reason for the lack of reference to the fraud-based loss allocation rule in the TILA and the CCA is

---

<sup>63</sup> See s. 525 comment d, s.526 comment c and s.531 comment c and comment f of the Restatement (Second) of Torts 1977. See the case of *Bernard Marko & Associates, Inc. v. Steele*, 230 So. 2d 42 (Fla. Dist. Ct. App. 3d Dist. 1970).

<sup>64</sup> *Master v Miller* (1791) 4 Term Rep. 320, at 329 per Lord Kenyon Ch J; *Co-operative Bank plc v Tipper* [1996] 4 All ER 366 *Teknik Cekap Sdn. Bhd. v Villa Genting Development Sdn. Bhd* 2000] 6 MLJ 513 at 529; *Holden v. Rutland Ry.*, 73 Vt. 317, 50 A. 1096, 1901 Vt. LEXIS 182 (1901).

<sup>65</sup> Section 134 of the TILA.

because they were drafted with the intention of providing the consumer with the necessary protection against the risk of fraudulent payment while balancing the interest of the issuer.<sup>66</sup>

In the case of the Malaysian EFT Guidelines, the loss allocation rules are already in favour of the issuer as seen from the rules which allocate losses based on the consumer's breach of duty to exercise reasonable care in relation to the access code and also the duty to strictly maintain the confidentiality of the access code or the electronic devices used to access the consumer's account. With these two bases of loss allocation, fraud is not necessary because the fraud rule as used in the TILA, the Banking Code and the CC Guidelines, clearly meant to strike a balance between protecting the consumer against unauthorised payment and at the same time, reducing the cost of misconduct by the consumer.

#### **4 COMPARISON AND CONCLUSION**

The discussion in this chapter has revealed another two loss allocation rules incorporated in the credit card and the EFT loss allocation schemes in the United States, United Kingdom and Malaysia. If in the previous chapter the loss allocation rules were discussed from the perspective of the mandate rule which concentrates on the

---

<sup>66</sup> *Office of Fair Trading v Lloyds TSB Bank plc* [2006] EWCACiv 268 and *Minskoff v. American Exp. Travel Related Services Co., Inc.* 98 F.3d 703, 708-709, C.A.2 (N.Y.), 1996.

application of the agency rules, in this chapter, the discussion focused on the allocation of unauthorised payment losses, based on the receipt of benefit rule, and fraud.

Some of the rules are generally identical in form but vary in detail. This variation is found not only in the cross jurisdictions analysis but across regulations in the same jurisdiction. The discussion has also shown that in some jurisdictions, the United States in particular, the rules are more detailed and are formulated, based on a broader range of principles.

The first part of this chapter analysed the rules which allow the issuer to allocate fraudulent payment losses to the consumer when there is lack of evidence pointing to the presence of a valid payment mandate from the perspective of agency rules. The rules which the issuer can apply as a basis for loss allocation in that circumstance is restitution for unjust enrichment and also fraud-based rule.

Loss allocation based on proof of the consumer's receipt of benefit from the disputed payment is incorporated only in the EFTA's and the TILA's loss allocation scheme. This rule, which as has been suggested, has its root in the law of restitution for unjust enrichment, changes the status of the unauthorised payment to an authorised payment if the issuer successfully proved that the consumer had received benefit from the payment.

However, the rule is not applicable in the United Kingdom and Malaysia since in these-

two jurisdictions, a claim in restitution for unjust enrichment can only be instituted against an immediate recipient but not a remote recipient. Regardless of that restriction, the issuer may rely on the agency of necessity rule or alternatively the “no profit of fraud” rule to bind the consumer to the disputed payment. Nonetheless, the application of these two rules is untested since so far, none of the UK Financial Ombudsman’s decisions refers to either of these rules. The position in Malaysia is, however, unknown because the decisions of the Mediation Bureau are not published to the public.

Another rule which describes the issuer’s right to allocate the losses from fraudulent credit card or EFT payments to the consumer, is the rule which requires the issuer to prove that the payment was fraudulently made by the consumer or by another person with whom the consumer was in cooperation.

There is no consistent policy across the three jurisdictions in relation to the fraud-based loss allocation rule. While in the United States the rule is applicable only to a dispute involving an EFT payment, or an EFT and charge card payment in the United Kingdom, in Malaysia, the rule is to be used to allocate fraudulent payment losses in a credit card payment only.

In the United States, fraud of the consumer is not used as a ground for allocating losses because the TILA was intended as a consumer protection statute. Since consumer fraud is more of a problem to the issuer, it is not taken as part of the TILA loss allocation scheme. The same policy is believed to be the basis of s.84 of the CCA where fraud is

not used as a basis for loss allocation. Nevertheless, from a business point of view, that attitude may affect the consumer because the issuer may raise the service fees in order to cover the cost of insuring against the consumer's own misconduct. However, as far as the TILA is concerned, the issuer may rely on the receipt of benefit rule to catch fraudulent consumers, provided it can show that benefit was received at the issuer's expenses.

The fraud-based loss allocation rule is used in the Malaysian credit card loss allocation scheme but not in the scheme for allocating losses caused by fraudulent EFT payments. The reason behind the different approach is perhaps to broaden the restricted scope of unauthorised payments in the CC Guidelines which referred only to a payment made "as a consequence of a lost or stolen credit card". Such a wider scope of loss allocation may be less important in the EFT Guidelines because it already has several bases for loss allocation, ranging from negligence to breach of strict duty of confidentiality. These rules give enough protection to the issuer to such an extent that it appears that the EFT Guidelines are intended to protect the issuer's interest instead of the consumer's.

Apart from the above rationale, the fraud-based loss allocation rule incorporated in the CC Guidelines also reflects the attitude of the drafters, which most probably was influenced by the payment industry players because of lack of pressure and participation by the consumer groups while in the United Kingdom and the United States, the rules were drafted with the participation of consumer representative bodies.

## PART II LOSS ALLOCATION AND THE BURDEN OF PROOF

### 1 INTRODUCTION

Another aspect of the loss allocation regulations that have an impact on the protection of the consumer against unauthorised credit card and EFT payment is the burden of proof. By burden of proof it means not only the person who has the onus to prove the alleged facts but also the facts to be proven.<sup>67</sup> Moreover, there is also the issue of the standard of proof which should be discharged to convince the court of the existence of the facts.<sup>68</sup>

The burden of proof rules in the various electronic payment regulations involved in this study described facts which the issuer, in most cases, has to prove to the satisfaction of the court, the Ombudsman or the Mediator before the disputed payment can be allocated to the consumer.

In the electronic payment systems' regulations discussed, the burden of proof is influenced by the use of complex electronic authentication methods.<sup>69</sup> Presumably, because the electronic payment system does not rely on a manuscript signature as an

---

<sup>67</sup> Chalmers, J., *Evidence* (2006), chp 2, at 7-8, Dundee University Press, (Hereafter Chalmers, J., *Evidence*), and Walker, A. G., *Law of Evidence in Scotland*, 2<sup>nd</sup> Edn (2000), at 11, para 2.11, T & T Clark.

<sup>68</sup> Chalmers, J., *Evidence*, at 12, 31A *Corpus Juris Secundum*, Evidence § 121, "Burden of proof properly so called" and also *Abrath v. The North Eastern Railway Company* (1882-83) L.R. 11 Q.B.D. 440 CA, at 449-452, per Brent M.R.

<sup>69</sup> Reed, C., "Consumer Electronic Banking" (1994) *J. I. B. L* 9 (11), 451-463, at 453 and Australian Securities and Investments Commissions EFT Working Group, "Discussion Paper on an Expanded EFT Code of Conduct", (July 1999) at <[http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/fineft.pdf/\\$file/fineft.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/fineft.pdf/$file/fineft.pdf)> at 26 (Visited 20<sup>th</sup> March 2005).

authentication method, the issuer's burden of proof is more technology oriented than the burden of proving the validity of a signature in the cheque payment system.<sup>70</sup> Therefore, unless the loss allocation schemes contain specific and clear rules regarding the parties' burden of proof, the issuer may, through its contract terms, require the consumer to prove certain facts. This contractual burden of proof may impose on the consumer the duty to show that the disputed payment was unauthorised instead of the issuer proving that the payment was authorised.

The impact of the reverse burden of proof is particularly harsh when both parties suffer from lack of evidence, as illustrated by the case of *Euro Cellular (Distribution) Plc. v. Danzas Ltd. T/A Danzas AEI Intercontinental*.<sup>71</sup> Although the case was not concerned with unauthorised payment, it is helpful in understanding the effect of lack of evidence on the contracting parties. In this case, a dispute arose as to the extent of the defendant's liability for the losses suffered by the plaintiff when two of their mobile phone consignments, which were kept at the defendant's warehouse, were lost. Both parties did not have clear evidence as to the cause of such loss. Their contract terms provided that if the loss proved to be the result of the defendant's negligence, his liability was unlimited. The contract also said that if the loss was caused by other than the defendant's negligence, the defendant's liability was limited. The question was who should be proving whether the defendant was entitled to the limited liability when evidence of the cause of the loss was unavailable.

---

<sup>70</sup> See the bank's burden of proof in case of forged cheque in *Barclays Bank Ltd v W. J. Simms* [1980] Q. B. 677, at 699.

<sup>71</sup> [2004] 1 Lloyd's Rep. 521.

Based on the construction of the contract and also for the purpose of justice, the court held that the defendant who wanted to rely on the limited liability provision must show that the loss was not caused by his negligence.<sup>72</sup> Eventually, because the defendant failed to discharge that burden of proof, the losses were allocated to him.

From this case, it is clear that the burden of proving or disproving the validity of the electronic payment has a significant impact in altering the allocation of loss from one party to the other. Hence, it is necessary to analyse the electronic payment systems regulations to identify the way the burden of proof is formulated. Some loss allocation rules may have been designed with a view of providing total protection to the consumer against the risk of fraud in the electronic payment system, without regard to the difficulty faced by the issuer in proving the validity of the payment in a complex electronic communication environment. Other rules may have taken that difficulty into account and allowed the issuer to rely on the presumption of authority, based on the proper functioning of the system. This type of rule allows the losses to be allocated to the consumer, based on the presumed validity of the payment mandate and not on clear evidence of authorisation.<sup>73</sup>

The burden of proof under all the electronic payment systems regulations discussed in this thesis is made up of various elements of proof. These elements in their totality

---

<sup>72</sup> Ibid, at 531.

<sup>73</sup> Geva, B., "Consumer Protection in Electronic Funds Transfers", Research Paper for Industry Canada/ Office of Affairs (March 2002) at <<http://www.osgoode.yorku.ca/gevapaper/gevaconspapermarch21.pdf>> at 28. (Visited 20<sup>th</sup> March 2005).



determine the party to whom the losses caused by the disputed payment should be allocated.

## **2 PROVING AUTHORISED PAYMENT**

### **A Proof of Authority to Initiate Payment**

All the regulations involved in this study, except the Malaysian CC Guidelines, impose on the issuer the duty to show that the disputed payment was authorised before it can claim a repayment from the consumer for the funds it has advanced for the respective payment.<sup>74</sup> The problem with the CC Guidelines is that although Para 13.3 of the Guidelines requires the issuer to show that the consumer had acted fraudulently or had failed to give a timely notice of loss or theft of the credit card, if it wishes to allocate to the consumer a bigger amount of losses than prescribed by Para 13.2, it did not explain the duty to prove the payment validity. Irrespective of that flaw, it is believed that the duty of a bank to prove that a debit to the consumer's account was authorised by the consumer is applicable since the Mediator should take into account the existing law in settling the dispute between the consumer and the issuer.<sup>75</sup>

---

<sup>74</sup> Section 909 (b) of the EFTA, s. 133 (b) of the TILA, s. 171(4) (b) of the CCA, Para. 14 (3) of the EFT Guidelines.

<sup>75</sup> See the Financial Mediation Bureau leaflet at <[http://www.fmb.org.my/pdf/leaflet\\_eng.pdf](http://www.fmb.org.my/pdf/leaflet_eng.pdf)> (Visited 12<sup>th</sup> April 2006).

Proving the validity of the disputed payment first and foremost requires the issuer to bring evidence to show that the access devices and/or the access code connected to the consumer's account was used either with actual authority or apparent authority.<sup>76</sup> In the case where it cannot prove that the payment was authorised, the issuer may allocate the losses to the consumer, provided it successfully proved the other elements required by the respective electronic payment systems regulations.

The issuer has to discharge his legal burden of proving the presence of the agency authority by a civil standard of proof. This standard of proof applies equally in the United States, United Kingdom and Malaysia.<sup>77</sup> However, in the United States, the standard of proof differs from one state to another. As a result, the level of protection enjoyed by the consumer may differ across the American states.<sup>78</sup> Some states give better protection than others because the issuer has a heavier burden of proof than a mere proof on the balance of probability.<sup>79</sup> For example, in the New Jersey decision in *Blaisdell Lumber Co. v. Horton*,<sup>80</sup> the Supreme Court required the merchant to establish apparent authority under the common law principle which is only on the balance of

---

<sup>76</sup> See *First Nat. City Bank v Mullarkey* 385 N.Y.S.2d 473, at 474; *Society Natl. Bank v Kienzle* 463 N.E.2d 1261, at 1265; *Bank of New York-Delaware v Santarelli* 491 N.Y.S.2d 980, at 1004. Section 133 (a)(1) (A) (E), s. 909(a) of the EFTA, s. 171 of the CCA, s. 12.12 of the Banking Code, and Para 14(3) of the Malaysian EFT Guidelines. See *Homburg Houtimport BV v Agrosin Private Ltd* [2004] 1 A.C. 715, at 725 the House of Lord decision relating to agency authority but not related to the payment systems.

<sup>77</sup> *Regina v. Hampshire County Council ex parte. Ellerton* [1985] 1 W.L.R. 749; *Lamb v. Lord Advocate* 1976 S.C. 110; *H M Shah Enterprise Sdn Bhd v Cecil Bernard Raman* [1998] MLJU LEXIS 1028; *Othman bin Abd Samad v Safety Life & General Insurance Sdn Bhd* [1996] 204 MLJU; *Ooi Poo Seng v Collector of Land Revenue, Kedah* [1994] 19 MLJU 1.

<sup>78</sup> See Mathews, M. E., "Credit Cards--Authorized and Unauthorized Use".

<sup>79</sup> See the different between the standard of preponderance of the evidence, the clear and convincing standard and beyond reasonable doubt standard in Lundy, T., "Jury Instruction Corner", (2003) 27-MAY Champion 61.

<sup>80</sup> 575 A.2d 1386 (N.J. Super. Ct. App. Div. 1990).

probability or preponderance standard, while in *Transamerica Insurance Co. v. Standard Oil Co.*<sup>81</sup> the North Dakota Court held that, “the party who alleges the existence of agency based upon apparent authority has the burden of proving that agency by clear and convincing evidence”.<sup>82</sup>

The North Dakota decision is beneficial to the consumer, in the sense that the issuer has a heavier burden of proof than in New Jersey since it must bring evidence which demonstrates a high probability of truth in comparison to proof by the preponderance standard, which is met when the “trier of fact ...thinks the chance greater than 0.5 that the plaintiff is in the right”.<sup>83</sup> In other words, to discharge the burden of proof on “clear and convincing” evidence, the issuer must convince the jury of the truth beyond the level of preponderance but not to the degree of beyond reasonable doubt.

Because of the different civil standard of proof required of the issuer, consumers in different state jurisdictions have different level of protection against unauthorised payment. In the state where the standard of proof is just the ordinary civil standard of probability, the issuer has a lighter burden to prove that the consumer is responsible for the disputed payment than in the state where the issuer has to prove the validity of the payment by clear and convincing evidence.

---

<sup>81</sup> 325 N.W.2d 210 (N.D. 1982), at 215-216.

<sup>82</sup> "Clear and convincing evidence is produced when the witnesses are found to be credible and their testimony is so clear, direct and weighty and convincing as to enable the jury to come to a clear conviction, without hesitancy, of the truth of the precise facts in issue. It is not required that the proof be voluminous or undisputed before it may be characterized as 'clear and convincing.'"

<sup>83</sup> *Brown v. Bowen*, 847 F.2d 342, 345-46 (7th Cir. 1988).

For instance, the Appeal Court in Louisiana applied the TILA's burden of proof in such a way that the consumer was faced with the duty to disprove an inference of authority, instead of clear proof of the payment validity. The case of *Cities Service Co. v. Paillet*<sup>84</sup> suffered from a lack of evidence as to the whereabouts of the credit card used to initiate the disputed payment and the identity of the party who initiated the payments. It was agreed that the card had been given by the defendant to be used by his employee for certain purchases only. However, the evidence did not show that the charges were made by the employee nor that the card was lost or stolen. Despite the inadequacy of evidence pointing to the loss, theft or wrongdoing which negates the validity of the payment and also to the fact that payment was initiated by the employee, the court held that the charges were authorised since the card was voluntarily transferred to the employee.

From this case it appears that the issuer can discharge his duty to prove the validity of the disputed credit card payment without bringing clear evidence that the payment was initiated by an authorised individual. What it has to do is to create an inference that since the card was not reported lost or stolen or somehow obtained by another through wrongdoing, the use was authorised. The decision in this case shows that the issuer's burden of proof can be discharged by merely creating an inference that the disputed payment was not unauthorised instead of showing that it was authorised. In this case, the consumer was required to bring evidence to show the card was used without authority to avoid the losses, i.e., by showing that the card was not used by an authorised individual or that it was lost or stolen. The standard by which the court allows the issuer

---

<sup>84</sup> 452 So.2d 319 La.App. 4 Cir.,1984

to discharge his legal burden of proving authorised payment contradicts the TILA rule which specifically imposed on the issuer the duty to show that the credit card was used by authorised individual, which in this case is the employee.<sup>85</sup>

The above cases show that although the TILA and the EFTA provide clear rules concerning the burden of proving the authority of the person who initiated the disputed payment, different standards of proof applied by the different American states may jeopardise the statutory protection of the consumer against unauthorised credit card or EFT payments.

The standard of proof which the issuer in the United Kingdom and Malaysia must discharge to show that the respective credit card or EFT payment is a valid payment is standardised because the courts uniformly apply the standard of proof on the balance of probability to a civil dispute.<sup>86</sup> The same standard of proof continues to apply even though the dispute between the consumer and the issuer is referred to the Financial Ombudsman in the United Kingdom and to the Financial Mediation Bureau in Malaysia.<sup>87</sup>

---

<sup>85</sup> Section 133 (b).

<sup>86</sup> See supra page 186, n 77 and the accompanying text.

<sup>87</sup> See the Financial Ombudsman News on Banking-Disputed Cash Withdrawal at <<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/25/25-banking-disputed-cash-withdrawals.htm>> (Visited 15<sup>th</sup> January 2006. See the Financial Mediation Bureau leaflet at <[http://www.fmb.org.my/pdf/leaflet\\_eng.pdf](http://www.fmb.org.my/pdf/leaflet_eng.pdf)> (Visited 15<sup>th</sup> January 2006) which mentioned that the mediator takes into account the existing law in the Mediation process.

**B      Proving the Functionality of the Access Device, Code and the Electronic Payment System Security as Proof of Payment Validity.**

This burden of proof rule is only applicable in the Malaysian EFT Guidelines. Paragraph 14 (3) and (4) of the Guidelines allow the issuer to discharge the burden of proving the validity of the EFT payment by bringing evidence to show that (i) the consumer's access device, access code and also the security of the EFT system was fully functional on the day in question; and (ii) that the employees or the agents of the issuer did not act fraudulently or negligently in carrying out the EFT payment.

This rule placed on the consumer the duty to bring evidence to rebut the presumption that the disputed EFT payment was authorised. To discharge this duty the consumer has to show that, despite the proper functioning of the access device or access code or the system in which the card and/or code was used, the payment was unauthorised. The consumer failure to discharge this evidential burden of proof means that the disputed payment is valid and he has to be responsible for.

The burden of proof rule in Para 14 (3) and (4) allocates the losses caused by fraudulent EFT payment to the consumer when he failed to defend himself against the issuer's evidence, particularly when the details of the system security can be kept secret from the

consumer if it “has direct relation to or impacts the security of the financial institution or its system.”<sup>88</sup>

The rule in Para 14 (4) also affects the consumer since the time frame for assessing the functionality of the systems is stated in term of the “day” when the disputed payment took place. Unless the issuer is required to prove that the disputed payment was made at the specific time when the system security was functioning, the rule allows the issuer to simply prove the general daily functionality of the system to allocate the losses to the consumer.

The effect of the rule in Para 14 (4) is even more damaging to the consumer if the EFT payment system is defined to include payment made via the internet.<sup>89</sup> Since in internet payment systems the threat of a security breach can come and go at any time of the day, and from many sources,<sup>90</sup> the consumer may be affected if the issuer is allowed to show that its systems are working properly while in reality, the fraudulent payment may have been facilitated by a security breach along the internet communication channel which neither the consumer nor the issuer was responsible for.

The same problem may occur if the payment is initiated via the m-payment system or any other telephone payment facility because the communication channel is not

---

<sup>88</sup> Paragraph 28 of the EFT Guidelines.

<sup>89</sup> See the definition of an Electronic Funds Transfer in Para 4 (f) of the EFT Guidelines which refers to among others a telephonic instrument. It is not clear whether this can be interpreted to refer to the internet.

<sup>90</sup> See Chapter Introduction at 2-3.

guaranteed safe from interference. However, it is believed that based on the definition of the EFT system in the EFT Guidelines, only a payment made via the m-payment system falls within the EFT Guidelines loss allocation scheme but not payment made through the internet, unless telephonic instrument in Para 4 (f) is interpreted to include the internet.<sup>91</sup> Nevertheless, the issuer of internet payment facilities may choose to insert Para 14 (4) conclusive evidence rule in its contract terms without committing an offence against the Payment Systems Act 2003 because it is not acting in contradiction of the EFT Guidelines.<sup>92</sup> Accordingly, the consumer cannot avoid the fraudulent payment if he cannot bring evidence to defend himself against the presumption that the internet EFT payment was authorised.

Apart from the above problems, Para 14 (4) (a) which considers the functionality of the card and the access code as proof of the payment validity may also affect the consumer since in some cases, neither of these items is needed to initiate an EFT payment. It is not uncommon to hear a news report of unauthorised payment made using a clone card when the consumer's details were stolen from a system break-in.<sup>93</sup> Because the issuer's evidence of the access device functionality is conclusive proof of the payment validity, the consumer may be made liable for the losses if he cannot bring evidence to show that the payment was not made using his access device. The consumer may face the same

---

<sup>91</sup> See Para 4 (f) of the EFT Guidelines which provides "For the purposes of these Guidelines, electronic fund transfer means fund transfers carried out through or by means of:... (f) telephonic instrument..."

<sup>92</sup> Section 57 of the Act.

<sup>93</sup> See for example Fox News "Security Breach May Put 40 Million Credit Card Holders at Risk" 18<sup>th</sup> June 2005 at <<http://www.foxnews.com/story/0,2933,159943,00.html>> (Visited 26<sup>th</sup> December 2005).



problem if the disputed payment was initiated with the use of an access code obtained by the fraudster as a result of a system security breach.

Finally, the consumer also faces a serious problem if he wants to disprove evidence which shows that the access card, code and the EFT system security were working properly since Para 14(4) (b) shows that the consumer must also bring evidence to disprove the issuer's evidence which showed that its officers or agents were not acting negligently or fraudulently in carrying out the EFT payment. Therefore, unless the word "and" at the end of Para 14 (4) (a) is interpreted to mean "or", the consumer must disprove both of the issuer's conclusive evidence in Para 14 before he can avoid the disputed payment.

From the discussion it is clear that the conclusive evidence rule in Para 14 (4) of the EFT Guidelines have several effects on the allocation of the fraudulent payment losses between the consumer and the issuer. In particular, it imposes an extremely difficult duty on the consumer to disprove the assumption of the payment validity while at the same time limits access to the material information, as the issuer is allowed to keep it confidential.

### **C      Proof of Receipt of Benefit**

Previously it was shown that under the EFTA and the TILA, the issuer has to prove the validity of the payment before it can claim a repayment from the consumer. It was also

mentioned that even if the issuer failed to prove the validity of the disputed payment, it could still allocate the losses to the consumer by showing that the consumer had received benefit from the disputed credit card or EFT payment.<sup>94</sup> It was suggested that the grounds of the claim in that circumstance is restitution for unjust enrichment.<sup>95</sup> To succeed in its claim, the issuer has to prove unjust enrichment by a preponderance of evidence unless it involves fraud where the standard of proof is higher.<sup>96</sup>

A common element of proving unjust enrichment in all the American states is that it is inequitable or unjust for the consumer to keep the benefit received from the issuer. However, that is only one part of the proof. Indeed, different states require proof of different other elements of unjust enrichment. For instance, in the states of Alaska, Utah, and Maine,<sup>97</sup> the claimant has to prove that the defendant knew about the benefit and that the benefit was conferred by the plaintiff upon the defendant. In some other states, knowledge of the benefit is not important. However, the issuer must show five elements of unjust enrichment namely, enrichment, an impoverishment, some connection between the two elements, the enrichment and impoverishment are not justified, and finally, the claimant has no legal remedy.<sup>98</sup> Finally, some states require

---

<sup>94</sup> Section 133 (b) of the TILA and s. 909(b) of the EFTA.

<sup>95</sup> See above page 157-165.

<sup>96</sup> *Matter of Estate of McKim* 111 N.M. 517, 807 P.2d 215 N.M.,1991; *Dolphin v. Wilson* 335 Ark. 113, 983 S.W.2d 113 Ark.,1998 and *Athey Products Corp. v. Harris Bank Roselle* 89 F.3d 430 C.A.7 (Ill.),1996 and *Collins Securities Corp. v SEC*, 562 F.2d 820, 823 (D.C.Cir.1977).

<sup>97</sup> *State Dept of Revenue, Child Support Enforcement Div. v Wetherelt* 931 P.2d 383 (Alaska 1997); *American Towers Owners Association, Inc v CCI Mechanical, Inc.*, 930 P.d 1182 (Utah 1996), and *Landry v Landry*, 1997 ME 173, 697 A.2d 843 (Me. 1997). See *Williston: A Treatise on Contracts*, §68:5.

<sup>98</sup> *Shroeder v Buchholz* 2001 ND 36, 622 N.W.2d 20 (N.D. 2001) and *Wilhite v Schendle* 92 F.3d 372 (5<sup>th</sup> Cir. 1996) applying Louisiana law. See Payne, A. M., and Leahy, M., "Restitution and Implied Contract", 66 *Am. Jur.* 2d § 12.

proof that the services provided by the issuer were valuable services; the consumer used and enjoyed the services and the issuer expected payment for those services.<sup>99</sup>

Obviously, since unjust enrichment is made up of different elements in different states' jurisdictions, the consumer's protection against the losses caused by unauthorised payment may also be affected. For example, in the states where proof of the consumer's appreciation or knowledge of the benefit is not required, the consumer's receipt of benefit will make him liable for the unauthorised payment even if he did not realise that the benefit came from the fraudulent use of his credit card, debit card and/or access code. On the other hand, in some states, the issuer must show not only that the benefit was conferred upon the consumer but it was used and enjoyed by the latter. In such a state, the issuer has a heavier burden of proof than just showing that it had conferred benefit upon the consumer.

Although the above differences may affect the uniform application of the TILA and the EFTA receipt of benefit rules across the United States, some might argue that the consumer should not be affected because the EFTA and the TILA loss allocation rules prevail over state law. However, it should be observed that the finality of the TILA and the EFTA rule requires, full understanding of the scope and the application of their rules. Unless there is a clear interpretation of the receipt of benefit rule; its scope and its application, it is hard to see how the different requirements of proving unjust enrichment

---

<sup>99</sup> *Shaw v Smith*, 964 P.2d 428 (Wyo. 1998), and *re Kellogg Brown & Root, Inc.*, 166 S.W.3d 732, 740 (Tex. 2005) (quoting *Vortt Exploration Co. v. Chevron U.S.A., Inc.*, 787 S.W.2d 942, 944 (Tex. 1990)).

may not affect the protection of the consumer against unauthorised payment. With due respect, the court in the case of *Citibank (South Dakota), N.A. v. Gifelman*<sup>100</sup> was presented with an opportunity to discuss and interpret the receipt of benefit rule but failed to do so. In fact, the decision suggested that the court treated any benefits connected to the unauthorised payment as the “benefit”, the receipt of which allows the issuer to allocate the disputed payment to the consumer even though the benefit was not the fruit of the unauthorised payment.<sup>101</sup>

In conclusion, it should be noted that the rule which allows the issuer to allocate fraudulent credit card or EFT payment to the consumer by proving that the latter had received benefit is not as straightforward as it first appears. Therefore, unless the court or the FRB produces a clear interpretation of the rule, its scope and its application, or that the issuer decides not to use the rule in the allocation of fraudulent payment losses, the consumer may be affected by the different elements of unjust enrichment which the issuer must prove in order to claim restitution from the consumer.

---

<sup>100</sup> 63 Conn.App. 188, 773 A.2d 993 Conn.App.,2001.

<sup>101</sup> See above at 161-163.

### 3 PROOF OF CONSUMER'S NEGLIGENCE OR FRAUDULENT ACTION AS AN EXCEPTION TO THE CAPPED LIABILITY

#### A Proof of Negligence

In the United Kingdom and Malaysia, the issuer can allocate unauthorised payment losses to the consumer if it can show that the payment was facilitated by the consumer's negligence.<sup>102</sup> Indeed, proof of negligence negates the capped liability limit prescribed by the Banking Code in the United Kingdom and by the EFT Guidelines in Malaysia.

The duty which conforms to the general burden of proof rule held in *Wilsher v Essex Area Health Authority*<sup>103</sup> that "the onus of proving causation lies on the pursuer" equally applies to dispute involving fraudulent EFT and also charge card payments in the United Kingdom by virtue of s.12.12. Moreover, it is to be noted that the rule continues to apply although the dispute has been referred to the Ombudsman.<sup>104</sup>

Apparently, since the Banking Code is not mandatory, the issuer may insert into its contract, terms which require the consumer to show that the payment was not caused by his negligence. Despite this possibility, it is believed that, based on the Ombudsman's

---

<sup>102</sup> Chapter three at pages 110-116 and 132-138.

<sup>103</sup> [1988] All ER 860, at 881 *per* Lord Bridge.

<sup>104</sup> Ombudsman's decision no. 25/13 at <<http://www.financial-ombudsman.org.uk/publications/Ombudsman-news/25/25-banking-disputed-cash-withdrawals.htm>>; See the Ombudsman view on this fact in "Using Plastic Cards As Credit-Tokens" <[http://www.financial-ombudsman.org.uk/publications/ombudsman-news/46/46\\_plastic\\_cards.htm](http://www.financial-ombudsman.org.uk/publications/ombudsman-news/46/46_plastic_cards.htm)> (Visited 26 December 2005).

decisions, the Banking Code rules always prevail over the contract terms.<sup>105</sup> Hence, any term that purports to shift the issuer's burden of proving negligence to the consumer is ineffective and unenforceable.

The same burden of proof is also imposed on the issuer by Para 15(1) (b) and (2) of the Malaysian EFT Guidelines. Although these provisions allow the issuer to allocate all of the disputed payment to the consumer if the consumer is proven to have acted negligently, they however failed to specify the party who should carry the burden of proving negligence. Apparently, Para 14 (3) provides that it is the issuer who has to show that the disputed payment was authorised before the consumer can be made responsible for it. However, since proving negligence is only required when the payment is unauthorised, the Para 14 (3) rule cannot be used to impose on the issuer the duty to prove the consumer's negligence. Apart from that flaw, Para 15 (1) (b) and (2) of the EFT Guidelines also failed to mention about proof of a causative link between the losses and the consumer's negligence like the one in s.12.11 of the United Kingdom Banking Code.

Nevertheless, the above weaknesses can be remedied by the general rule of negligence which imposed on the person alleging negligence the duty to show that his losses were caused by the defendant's negligence.<sup>106</sup> Indeed, in *Lim Soh Wah & Anor v Wong Sin*

---

<sup>105</sup>See the Ombudsman's decision at <<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/9/sept-disputed-cash-machine-withdrawals.htm>> (Visited 26th November 2005).

<sup>106</sup> *Kian Lup Construction v Hongkong Bank Malaysia Berhad*, [2002] 252 MLJU 1, at 42-43.

*Chong & Anor*<sup>107</sup> it was explained that, “A plaintiff may suffer damages. But it is of no consequence unless the defendant negligently caused it. If the damage would have happened anyway, then the defendant cannot be held liable for it. For liability to be visited upon a defendant's head it must be proved that but for his negligence the harm would not have happened.”<sup>108</sup>

In conclusion, it can be said that the party who bears the burden of proving negligence in the Malaysian EFT Guidelines is the issuer. Furthermore, the issuer must also show that there is a causative link between its losses and the consumer's negligence. This burden of proof rule should apply even though a dispute involving unauthorised electronic payment is referred to the Mediation Bureau because the Mediator must take into account the applicable law in its Mediation process.<sup>109</sup>

## **B Proof of Fraud**

Another aspect of the loss allocation scheme found in all three jurisdictions is an allocation of fraudulent payment losses based on consumer fraud. This rule is used by the EFTA, the Banking Code and the CC Guidelines.<sup>110</sup>

---

<sup>107</sup> [2001] 2 CLJ 344.

<sup>108</sup> *Ibid*, per Gopal Sri Ram JCA, at 347.

<sup>109</sup> The Financial Mediation Bureau leaflet at <[http://www.fmb.org.my/pdf/leaflet\\_eng.pdf](http://www.fmb.org.my/pdf/leaflet_eng.pdf)> (Visited 15<sup>th</sup> January 2006).

<sup>110</sup> Section 903(11) (B) of the EFTA, s. 12.12 of the Banking Code and Para 13.2 and 13.3 of the CC Guidelines.

Basically, the rule requires the issuer to prove that the consumer had acted fraudulently in relation to the disputed payment before it can allocate to the consumer a bigger amount of losses than the capped liability limited to the consumer.

It should be noted that the standard of proving fraud in different jurisdictions varies. Even different American states apply different standards of proving fraud. For instance, in states such as New Jersey, Iowa and Maryland, the issuer must prove fraud by false representation with clear and convincing evidence.<sup>111</sup> On the other hand, states such as Tennessee require proof by preponderance of evidence.<sup>112</sup>

The duty to prove fraud under the EFTA may also cause a problem since the element of fraud required to be proved differs across the states' jurisdictions. In some states, the plaintiff must show that the consumer had committed fraud with the intention to deceive while in some other jurisdictions, the issuer needs to prove that the consumer intended his false representation to be relied on.<sup>113</sup> Nevertheless, taking the differences into account, s. 909(11) (B) of EFTA described fraud as fraud committed with fraudulent intent. In other words, for the consumer to be liable to the issuer for the disputed EFT payment on ground of fraud the issuer must prove that the consumer had acted with the

---

<sup>111</sup> *Albright v. Burns*, 206 N.J. Super. 625 (App. Div. 1986); *Intile Realty v. Raho*, 259 N.J. Super., 438 (Law Div. 1992); *Stochastic Decisions v. DiDominico* 236 N.J. Super. 388 (App. Div. 1988); *Loyola Fed. Sav. and Loan Ass'n v. Trenchcraft, Inc* 17 Md.App. 646, 303 A.2d 432 Md.App. 1973; *Sjostrand v. North Dakota Workers Compensation Bureau* 649 N.W.2d 537 N.D., 2002

<sup>112</sup> *Gentry v. Hill*, (Tenn. Ct. App. Sept. 25, 1985); *Mary Jarmakowicz v Billy Suddarth* No. M1998-00920-COA-R3-CV.Feb. 28, 2001. See (1968) 37 *Am.Jur.*2d, Fraud and Deceit, ss. 107 and 113.

<sup>113</sup> See 37 *Am. Jur.* 2<sup>nd</sup>, Fraud and Deceit ss. 107 and 113.



intention to deceive.<sup>114</sup> By specifically referring to fraudulent intent, the rule promotes uniform application of the EFT loss allocation scheme in all the American states.

In the United Kingdom, the Banking Code also allocates losses based on fraud and requires the issuer to prove the presence of the consumer's fraud. However, it did not specify the standard of proof to be used in the process. As such, the standard of proving fraud on the balance of probability, which is applicable in the civil proceeding, should be applied by the Ombudsman.<sup>115</sup> In *Bohar Singh Khera v Secretary of State for the Home Department*,<sup>116</sup> Lord Bridge of Harwich, with whom Lord Templeman expressed agreement, concluded: "the civil standard of proof by a preponderance of probability will suffice, always provided that, in view of the gravity of the charge of fraud which has to be made out and of the consequences which will follow if it is, the court should not be satisfied with anything less than probability of a high degree."

The standard of proving fraud in credit card payment in Malaysia is, however, unsettled. There are two contradictory standards of proof used in Malaysia. In the case of *Lau Hee Teah v Hargill Engineering Sdn Bhd & Anor*<sup>117</sup> it was held that the plaintiff has to prove fraud on the balance of probability. However, it added that the degree of probability which must be established varies from case to case, depending on the gravity of the allegation. This standard of proof is similar to the position in the United Kingdom

---

<sup>114</sup> See Chapter four at 173-175.

<sup>115</sup> *Credit Lyonnais Bank Nederland NV v. Export Credits Guarantee Department* [1999] C.L.C. 823.

<sup>116</sup> [1984] A.C. 74, at 124. The standard was upheld by the Court of Appeal in *Regina (N) v. Mental Health Review Tribunal (Northern Region) and others* [2006] 2 W.L.R. 850, at 864.

<sup>117</sup> [1980] 1 MLJ 145, at 150.

mentioned earlier. Six years after that case, the Supreme Court in *Chu Choon Moi v Ngan Sew Tin*<sup>118</sup> held that a fraud claim, whether raised in civil or criminal proceedings, must be proved beyond reasonable doubt; which is referred to as proof of a high degree of probability.

The hierarchy of the Malaysian court caused serious confusion as to which of the two standards of proof is to be applied. At one time, the Federal Court was the highest court of the land until it was renamed the Supreme Court in 1985. Later in 1994, the court was again renamed the Federal Court. Since both courts applied different standards of proof of fraud, while each was the higher court of the land, it is difficult to figure out which of the standards should be applied in a dispute involving fraudulent credit card payment. Reported cases show that some of the courts follow the Federal Court's decision<sup>119</sup> while other follows the Supreme Court's decision.<sup>120</sup>

Despite the uncertainty, it is believed that the issuer should be required to present the highest proof possible in order to allocate the losses to the consumer. Even if the standard is not as high as in criminal cases, a higher degree of evidence should be brought by the issuer to prove the consumer's fraudulent action since an allegation of fraud affects not only the allocation of the disputed payment losses but also the consumer's credit reputation.

---

<sup>118</sup> [1986] 1 MLJ 34, at 38.

<sup>119</sup> *Hock Hua Bank (Sabah) Bhd v Lam Tat Ming & Ors* [1995] 4 MLJ 328; *Daro (M) Sdn Bhd v Chan Tse Yuen & Others* [2002] 376 MLJU 1.

<sup>120</sup> *SAZ Corporation Sdn Bhd v Besin Sdn Bhd and Anor* [2004] 615 MLJU 1.

#### **4      PROOF OF PRE-CONDITIONS FOR ALLOCATING LOSSES TO THE CONSUMER**

The consumer apparently, has a duty to prove the validity of the disputed payment or, in the case where the payment is unauthorised, to show that the consumer is nevertheless responsible for the disputed payment because of the receipt of benefit rule or the tort of deceit rule. However, in case the issuer cannot prove either of the above and the payment falls under the description of unauthorised payment, the consumer may still allocate the capped liability limit to the consumer if the issuer successfully proves that the underlying conditions that set the foundation for the issuer's right to allocate the unauthorised payment to the consumer have been met.<sup>121</sup>

It should be noted that some of the conditions apply only to the loss allocation under the TILA and the EFTA while others apply to all the regulations involved in this study.

##### **A      Proof of Acceptance of the Access Device or Code**

The EFTA and the TILA require the issuer to show that the card or the means of accessing the consumer's account was an accepted card or code before any disputed payment can be allocated to the consumer.<sup>122</sup> The same condition is incorporated in the

---

<sup>121</sup> See s. 133(a)(1)(A)-(F) of the TILA and s. 909 (a) of the EFTA.

<sup>122</sup> Section 133(a)(1)(A), s. 103(l) of the TILA and s. 226.12(a)(2) of Reg. Z and s. 909(a), s. 903(1) of the EFTA and s. 205.2(2) of Reg. E.

CCA and the Banking Code in the United Kingdom and also in the Malaysian EFT Guidelines.<sup>123</sup>

All the regulations reviewed in this study refer to an accepted card as a card either requested”, “received”, “signed” or used”.<sup>124</sup> These terms indicate more than mere receipt of the card and/or the code but refer to a conscious act of either the card holder himself or a person authorised by him.<sup>125</sup> Hence, when the card or the access code is used by the consumer or its authorised user, the consumer actually accepts the responsibility and duty as a principal. At the same time, the issuer becomes an agent to the consumer when the issuer processes and executes the payment as instructed by the consumer or the authorised user of the card and/or code.<sup>126</sup>

Another argument for setting the acceptance of the card and/or code as a condition for allocating the losses to the consumer is found in contract law. A card and /or a code which is not used by the consumer or its authorised user cannot create an agency relationship between the consumer and the principal because the agency relationship arises out of an agreement between the principal and the agent. When the card is offered to the consumer by the issuer but not accepted, no contract is created because there is no

---

<sup>123</sup> Section 66, and s. 171 (4) (a) of the CCA, s. 12.12 of the Banking Code and Para 17 (2) of the Malaysian EFT Guidelines.

<sup>124</sup> See above nn 122 and 123.

<sup>125</sup> Goode, R. M., *Consumer Credit Law and Practice* Issue 12, para 126.

<sup>126</sup> Hapgood, M. (Ed) *Paget's Law of Banking*, 12<sup>th</sup> Edn (2002), para 17-163, Butterworths Lexis Nexis and Hooley, R. and Taylor, J., “Payment by Funds Transfer” Ch. 3 in Brindle, M. and Cox, R., *Law of Bank Payments*, at 3-067.

*consensus ad idem*.<sup>127</sup> Because there is no contractual relationship between the consumer and the issuer, they do not owe one another contractual rights and duties as principal and agent.<sup>128</sup> Consequently, when the issuer receives a payment instruction from a person who is not authorised to receive the card and/ or code and the instruction is issued with the use of those items, the issuer is not authorised to act as an agent for the consumer in making a payment from the consumer's account. As a result, the consumer is not responsible for that payment.

The TILA accepted card rule was applied in many cases including *American Nat. Bank of Beaumont v. Rathburn*.<sup>129</sup> The dispute in this case involved the use of a credit card by the defendant's wife who, after their separation, took the card without the defendant's knowledge. Evidence showed that the card was sent as a promotional package to the defendant. However, the defendant never expressly or implied authorising the wife to use the card. The issuer failed to prove that the card was an accepted card. Therefore, the court held that the issuer could not allocate the losses to the consumer because it failed to fulfil the condition set by s.133 (a) (1) of the TILA.

---

<sup>127</sup> Sections 1, 17, 22 and 24 of the Restatement (Second) of Contract 1981; s. 2 (a) (b) of the Malaysian Contracts Act 1950; Furmston, M. P. (Ed), *Cheshire, Fifoot and Furmston's Law of Contract*, 14<sup>th</sup> Edn. (2001), at 29-43, Butterworths. See Howard, M., "Shifting Risk and Fixing Blame: The Vexing Problem of Credit Card Obligations in Bankruptcy", (2001) 75 *Am. Bankr. L.J.* 63, at 68. See Restatement (Second) of Contracts, s. 31 (1981)

<sup>128</sup> In the case of *Pole v. Leask* (1863) 33 L.J. Ch. 155, at 161, *per* Lord Cranworth, it was held that, "No one can become the agent of another person except by the will of that person." Similarly, in *Garnac Grain Co. Inc. v. H. M. F. Faure & Fairclough Ltd*, [1968] A.C. 1130, at 1137, *per* Lord Pearson it was held that the relationship of principal and agent can only be established by the consent of the principal and the agent."

<sup>129</sup> 264 So. 2d 360 (La. App.. 1972) at 262-263. At this time section 132 was not inserted in TILA yet. It appears that if it was, the issuer would have been liable for violating the TILA by sending an unsolicited credit card to consumer.

The same burden of proof has to be discharged by the issuer in a dispute involving the validity of an EFT payment. In the case of *Ognibene v. Citibank, N.A.*,<sup>130</sup> which concerned unauthorised use of a cash card, the court held that since the issuer had failed to show that the means of access used in the disputed transaction was accepted by the consumer under s.903 (1) of the EFTA, none of the losses could be allocated to the consumer.

In Malaysia, the accepted card rule is incorporated in the loss allocation scheme for the EFT payment system but not in the credit card system. The reason behind such an approach is not clear. It is perhaps sensible to suggest that because the CC Guidelines restrict the issuance of the credit card to the applicant, the rule which is intended to protect the consumer from the risk of an unauthorised payment involving a credit card sent in a promotional package is unnecessary.<sup>131</sup> However, such an approach is questionable because a cash card or a debit card is also issued at the request of the consumer but the EFT Guidelines clearly provide that if a dispute arises concerning the consumer's card, the consumer is presumed not to have received the card unless the issuer can prove otherwise.<sup>132</sup> Like the EFT Guidelines, the CC Guidelines too should contain this rule because it helps to protect the consumer in circumstances where his identity is fraudulently used to apply for a credit card facility.

---

<sup>130</sup> 12 Misc.2d 219, 224, 446 N.Y.S.2d 845 848, N.Y.City Civ. Ct.,1981.

<sup>131</sup> Weistart, J., "Consumer Protection in the Credit Card Industry: Federal Legislative Controls", at 1523-1525. Part Two of the Credit Card Guidelines.

<sup>132</sup> Paragraph 17(2) of the EFT Guidelines.

## **B Proof of Issuance of an Identification Method**

The duty to show that the consumer or other authorised user has been provided with an identification method is only found in the EFTA and the TILA loss allocation schemes. Section 909 (a) of the EFTA and s. 133 (a) of the TILA clearly say that the identification method is required so that “the user of such card [code, or other means of access] can be identified as the person authorized to use it.” It was mentioned earlier that the electronic payment systems depend on various new methods of authenticating the payment instruction since a manual transcript signature most of the time is not suitable for use.<sup>133</sup> Since the system is developed by the issuer, it is the best party to undertake research and to invest in innovating and developing a suitable method of authenticating the authority of the person to initiate a credit card or EFT payment in a particular commerce system.<sup>134</sup>

The requirement on the issuer to provide an identification method is not unique since it was already applied by the court even before the EFTA and the TILA were passed. In the case of *Lit Bros. v. Haines*,<sup>135</sup> for instance, the consumer became a store credit account holder and was given an identification coin bearing a number corresponding to her account number. This coin allowed the consumer to make purchase at the issuing store. However, it did not have any authentication feature other than the account

---

<sup>133</sup> See Chapter two at 41.

<sup>134</sup> See Cooter, R. D., and Rubin, E. L., “A Theory Of Loss Allocation For Consumer Payments”, who suggested that based on the loss spreading and loss reduction principles the losses would be allocated to the issuer for failure to innovate.

<sup>135</sup> 98 N.J.L. 658 (N.J. Sup. Ct. 1923).

numbers and the account holder's name and address. When the coin was stolen and used to make an unauthorised purchase, the consumer refused to pay. The court found for the consumer and held that unless there was an express agreement to the contrary, a coin issued to a store account holder served only as an identification method but not as a method of authenticating the authority of the user to initiate the disputed payment.<sup>136</sup>

The above opinion is now part of the TILA and the EFTA loss allocation rule and its application can be found, for instance, in the case of *Kruser v Bank of America*<sup>137</sup> where the court while interpreting s.909 (a) of the EFTA stressed that the consumer is responsible for the EFT payment if the access device used to initiate the payment was an accepted device and the issuer had provided the consumer with an identification method. However, if the issuer failed to provide the identification method it lost the right to allocate even the prescribed capped liability amount of losses to the consumer.<sup>138</sup>

Literal reading of the rule, which requires proof that the issuer had provided the consumer with an identification method, suggests that in a distance contract through m-commerce or internet commerce systems, where neither the card nor a signature, a photograph or a PIN can authenticate the authority of the person who issued the payment mandate, the issuer may allocate the unauthorised payment to the consumer by proving that the consumer was provided with an identification method. It does not matter whether the method is suitable for the particular commerce system or not.

---

<sup>136</sup> See also *Sears, Roebuck & Co. v. Duke* 441.S.W2d 521 Tex 1969.

<sup>137</sup> *Kruser v. Bank of America* 230 Cal.App.3d 741, 281 Cal.Rptr. 463 Cal.App. 5 Dist., 1991.

<sup>138</sup> *Crestar Bank, N.A. v. Cheevers* 744 A.2d 1043, 1049 (D.C. 2000)



Nevertheless, if the rule is read in the light of the function of the identification method as described by the EFTA, the TILA and their accompanying regulations, Reg. E and Reg. Z respectively which is a means of identifying the person who issues the payment mandate via the card, code or other means of accessing the account,<sup>139</sup> the rule requires more than a mere supply of the identification method. Therefore, it is not enough that the consumer was given an identification method but that the method must be able to function properly in the type of transaction in which the card or the means of accessing the account are used.

The functional interpretation of the rule was explained by the court in the case of *Crestar Bank N.A. v Cheever*<sup>140</sup> In this case, the disputed payment took place at a vending machine. Evidence showed that the vending machine where the transaction took place could not authenticate the authority of the card's user as it neither accepted a photograph nor a signature. Based on this evidence, the court held that the issuer had failed to discharge its burden of proving that the consumer was provided with an identification method that would work at a vending machine. Consequently, by virtue of s.133 (a) of the TILA, the issuer cannot allocate the losses from the disputed payment to the consumer.

The Federal Reserve Board was also of the view that in the case where the necessary identification method, either the card itself or another means of identification was not

---

<sup>139</sup> Section 909(a) of the EFTA, s. 205.6(a) of Reg. E, s.133(a)(1)(F) of the TILA, and s.26.12 (b)(2)(iii) of Reg.Z

<sup>140</sup> *Crestar Bank, N.A. v. Cheevers*, 744 A.2d 1043 (D.C. 2000), at 1049.

functioning at the moment the payment was initiated, the issuer cannot rely on the TILA capped liability rule to allocate any of the losses to the consumer, not even the TILA's capped amount of liability.<sup>141</sup> The same comment should apply to the rule in s. 909 of the EFTA.

The burden of proving that the consumer was issued with an identification method is helpful to protect the consumer in cases where the unauthorised transaction was made using the consumer's credit card or account details in a distance contract via the internet, m-commerce system, and telephone shopping. Until the issuer can develop a suitable and effective means of authenticating the authority of the person who initiated the payment in that environment, the consumer is protected from the losses.

This condition which underlines the issuer's right to allocate unauthorised payment losses to the consumer is neither incorporated in the loss allocation scheme in the United Kingdom nor in Malaysia. Considering the benefit of the rule which sits as a condition precedent to the issuer's right to allocate the fraudulent payment losses to the consumer, which is a last resort for the protection of the consumer, in the event, other conditions of liability if proved, it is regrettable that it is not incorporated in the UK and the Malaysian loss allocation schemes. In particular, the consumer loses a higher level of protection in those circumstances where the issuer, for profitable gains, allowed the payment facility to be used in the commerce system while the consumer for convenience and also necessity, has to face the risk of an unauthorised payment from uncertain and unknown

---

<sup>141</sup> Official Staff Commentary to TILA Para 12.b (2)(iii).

security threats. The requirement for the issuer to prove the issuance of the identification method corresponds to the idea that when the issuer is the best person to prevent the losses, it should be responsible for the losses if it failed to innovate and produce a system that can prevent or reduce the risk of fraudulent payment.<sup>142</sup>

### **C      Warning of Potential Liability**

The third condition which the issuer must prove before it can allocate fraudulent payment losses to the consumer is that it had warned the consumer of the consumer's potential liability if unauthorised credit card or EFT payment occurs.

Section 133 (a) (1) (C) of the TILA and s. 905 (a) (1) of the EFTA provides that an issuer must give an adequate notice of potential liability to the consumer before the prescribed maximum amount of liability may be allocated to the consumer.<sup>143</sup> The purpose of the notice is to educate the consumer about the kind of risk associated with the credit card or the EFT payment facility. By giving this notice, it is hoped that the consumer understands the important link between the risk of an unauthorised payment and his liability for failure to take the required action to prevent or reduce the risk.<sup>144</sup>

---

<sup>142</sup> *Supra* n 134.

<sup>143</sup> Section 205.6 (a) and s. 205.7 (b)(i) of Reg. E and S.26.12 (b)(2)(ii) of Reg. Z.

<sup>144</sup> In fact it was said that a person's responsiveness to a liability rule depends on his knowledge of the rule and his abilities to consider the rule when fashioning his –behaviour. See Reilly, M. T., "The FDIC As Holder In Due Course: Some Law And Economics", (1992) *Colum. Bus. L. Rev.* 165 at 204

What is regarded as adequate notice, according to footnote 23 to section 226.12 (b)(2)(ii) of the Regulation Z, is “a printed notice to a card holder that sets forth clearly the pertinent facts so that the card holder may reasonably be expected to have noticed it and understood its meaning.” The notice must specify the maximum limit of loss to be allocated to the consumer as long as it is not in excess of the \$50 limit prescribed by section 133(a)(1)(B) of the TILA. The disclosure can be done in the initial disclosure required by section 226.6 of the Reg. Z; on the credit card itself or on the periodic statement sent to the consumer, provided it is given before the unauthorised use occurred.<sup>145</sup> It was held in *First Nat. City Bank v. Mullarkey*<sup>146</sup> that the conditions of liability that the issuer has the burden to meet include giving adequate notice of the potential liability to the consumer.

The same requirement can be found in the Malaysian CC and EFT Guidelines. Paragraph 6(4) (a) of the EFT Guidelines impose on the issuer the duty to warn the consumer of his potential liability for any unauthorised payment. However, Para 13.5 of the CC Guidelines require the issuer to warn the consumer of potential liability if he acts fraudulently or fails to notify the issuer of the loss or theft of the credit card.

Apparently, the rules in both guidelines use the word “shall” which connotes either a compulsory or directory rule. Since s 57 of the Payment Systems Act 2003 made it an offence for the issuer to act in contradiction of the Guidelines, the rule is mandatory in

---

<sup>145</sup> Staff Commentary to Regulation Z, Para 12(b)(2)(11)

<sup>146</sup> 385 N.Y.S.2d 473 1976, at 474. In this case the court held that the conditions of liability that the issuer has to prove include giving adequate notice of potential liability to the card holder.

nature.<sup>147</sup> Nevertheless, the issuer's failure to comply with the rule is not prejudiced to its contractual right to allocate fraudulent payment losses to the consumer because the Guidelines and the Payment Systems Act did not render such an agreement unenforceable.

The issuer of a credit card in the United Kingdom is also required by s. 60(1)(a) of the CCA to disclose to the consumer his rights and duties under the agreement and also the protection and the remedies as provided by the Act.<sup>148</sup> Part I of Schedule 2 of the Consumer Credit (Agreements) Regulations 1983 shows that the disclosure includes a warning of the consumer's potential liability in circumstances like loss, theft or misuse of the card or use of the card with the consumer's consent.

It should be observed that if the issuer failed to comply with this section, the agreement becomes an improperly executed agreement under s.61 of the CCA.<sup>149</sup> As a result, the issuer cannot enforce the agreement except with an order from the court.<sup>150</sup>

Obviously, the CCA disclosure becomes a condition which the issuer must fulfil before it can allocate fraudulent payment losses to the consumer. However, it does not totally prevent the issuer from claiming repayment from the consumer. What happens is the consumer continues to be liable for the fraudulent payment provided the conditions that

---

<sup>147</sup> *Cheong Seok Leng v Public Prosecutor* [1988] 2 MLJ 481, at 489, *Muip Bin Tabib v Dato James Wong; Wan and Hamid Bin Tuanku Surur v Francis Loke*, [1971] 1 MLJ 246, at 249.

<sup>148</sup> Section 60(1)(a)(c) of the CCA.

<sup>149</sup> Section 61(1)(a) of the CCA.

<sup>150</sup> Section 65(1) and s. 127 of the CCA.

trigger the liability are met. Nonetheless, the lack of disclosure means that he does not have to repay the issuer for the fraudulent payment since the improperly executed agreement prevents the issuer from claiming the remedies, unless the court allows such a claim.<sup>151</sup>

Apparently, the disclosure requirement in s. 61(1)(a) of the CCA is not as strict as the EFTA and the TILA rules which completely prevent the issuer from allocating the disputed payment to the consumer if the agreement did not contain a warning of the consumer's potential liability.

Nonetheless, the issuer of a charge card may have failed to disclose the consumer's potential liability but be unaffected by the rule in s.61 and s. 65 of the CCA because the charge card agreement is an exempt agreement.<sup>152</sup> Similarly, the debit card issuer is not prevented from allocating the losses to the consumer if other conditions for liability are satisfied simply because it had failed to warn the consumer of the potential liability since an agreement for the issuance of a debit card is not a regulated agreement that falls under s.61 and s. 65 of the CCA.<sup>153</sup>

---

<sup>151</sup> *R. v Modupe* [1991] Crim.L.R. 531.

<sup>152</sup> Section 16 (5)(a) of the CCA and art. 3 (1)(a)(ii) of the Consumer Credit (Exempt Agreements) No.2 Order, SI 1985/757.

<sup>153</sup> Ellinger, E. P. *et al*, *Ellinger's Modern of Banking Law*, 4<sup>th</sup> Edn. (2006), 599-601, Oxford University Press and Smith, M. and Robertson, P., "Plastic Money", Brindle, M. and Cox, R., *Law of Bank Payments*, paras 4-064- - 4-071.

## **D Proof of the Disclosure of the Notification Method**

All the regulations, except the Banking Code, require the issuer to inform the consumer of the method to be used to inform the issuer of an unauthorised payment or the events that may lead to unauthorised payment.<sup>154</sup>

The rule, however, varies across the regulations. The TILA allows the details to be given, either on the face or reverse side of the periodic statement of balance,<sup>155</sup> on a separate notice sent together with the statement or even orally, as long as it was given before the disputed unauthorised payment occurred.<sup>156</sup> The timing is very important because the purpose of the notice is to enable the consumer to take steps to prevent or reduce losses due to unauthorised use.<sup>157</sup> On the other hand, the EFTA requires the issuer to inform the consumer of the method of notification in the initial disclosure given to the consumer at the time of contracting for the services or before the first EFT payment is initiated.<sup>158</sup>

The issuer's failure to show that the notification details have been provided to the consumer is fatal to his right to allocate the unauthorised payment losses to the

---

<sup>154</sup> Section 133(a) (1) (D) of the TILA, s. 226.12 (b)(2)(ii) of Regulation Z, s.905 (a)(1)(2) of the EFTA, s.205.7(a)(b)(1)(2) of Reg. E and Para 205.7 (a)(1) of the Staff Interpretations, s. 84 (4) of the CCA, Para 6(4)(b) of the EFT Guidelines, and Para 13.1 CC Guidelines.

<sup>155</sup> Section 127(b) of the TILA. *Broadwick Financial Services Limited v. David John Spencer, Sylvia Julie Spencer* [2002]EWCA Civ 35 CA.

<sup>156</sup> Section 133(a)(1)(D) of TILA; Official Staff Commentary Para 12(b)(2)(ii) to Regulation Z stated that the information required by section 133(a)(1)(D) can be disclosed to the card holder in the "initial disclosures under section 226.6, on the credit card itself, or on periodic statements".

<sup>157</sup> *Supra* n 134.

<sup>158</sup> Section 205.7 (a) of Reg. E.

consumer. For instance, in the case of *Thomas v Central Charge Service, Inc.*<sup>159</sup> it was decided that the consumer could not be made liable for the unauthorised payment that occurred because the contract between the parties failed to specifically require the consumer to notify the issuer of the loss or theft of the card.

Although the rule is advantageous to the consumer, it is not up to date with the current internet communication revolution. In this age where many banks and credit institutions are offering online services, the rule should be amended to offer an electronic means of communication which should include an e-mail facility or a specific web form for notification. However, before the issuer can use the internet or mobile communication technology for the disclosure, the issuer must obtain the consumer's consent as required by s. 101(c) (1) of the Electronic Signatures in Global and National Commerce Act 2000 ( the "ESign").

It should be noted that in the United Kingdom, the CCA in s 84 (4) requires the issuer to give a notice to the consumer informing the latter of the name, address and telephone number of its staff to whom the consumer should call about the loss, theft or potential misuse of the credit card. This rule resembles the EFTA and the TILA rules because it also works as an underlying condition for the issuer's right to allocate any of the losses from fraudulent credit card payment or misuse of the card to the consumer. Nevertheless, it is not clear whether the condition applies in the case of a fraudulent payment made in a distance transaction. Most probably, the issuer need not describe the

---

<sup>159</sup> 212 A.2d 533 D.C.App. 1965, at 534.



mode of notification to the consumer because s.84 (3A) prevents the issuer from allocating the losses incurred in the distance transaction to the consumer. In this circumstance, it is not necessary to impose on the issuer the duty to disclose the notification method to the consumer since failure to notify is not a condition for allocating the losses to the consumer.

In Malaysia, only the EFT Guidelines contain a rule which requires the issuer to specify the method of notification of an unauthorised or potential unauthorised payment in the contract terms.<sup>160</sup> This requirement is mandatory.<sup>161</sup> Nevertheless, unlike the position in the United States and the United Kingdom, the issuer is not barred from allocating the losses caused by a fraudulent EFT payment to the consumer even if the issuer failed to perform this duty.

Although the United Kingdom Banking Code and the Malaysian CC Guidelines do not require disclosure of a notification method, it is believed that for consumer protection purposes and also for efficient allocation of loss, the issuer should disclose to the consumer the method of notification. In fact, the consumer should be told of the method of notification, irrespective of the medium in which the payment is initiated since notification of an unauthorised payment or a potential unauthorised payment is helpful to prevent or reduce losses.<sup>162</sup> Moreover, because the Banking Code and the CC Guidelines impose on the consumer the duty to inform the issuer of the events which

---

<sup>160</sup> Paragraph (4) (a) of the EFT Guidelines.

<sup>161</sup> See above page 212-213 and n 147.

<sup>162</sup> Supra n 134.

may facilitate unauthorised payment before he can claim protection against loss, it is fair that the consumer is informed of the method to be applied to give effective notification. The information will encourage timely notification which is advantageous to the issuer as it gives the issuer the necessary information to enable it to take action to prevent or reduce the losses.

## **5      COMPARISON AND CONCLUSION**

In this chapter, it was shown that the burden of proof has a significant impact on the protection of the consumer against unauthorised payment losses. The rule concerning burden of proof determines not only the party responsible to prove the presence of the facts, but also of satisfying the standard of proof of the facts, in order to show that the losses should be allocated to the consumer. Apart from that, it was also revealed that the issuer must fulfil certain underlying conditions before it can use its right to allocate the disputed payment to the consumer.

A person to whom the burden of proof is allocated faces the possibility of bearing the losses if he cannot discharge that burden. Accordingly, if the consumer is required by the loss allocation rule to prove the invalidity of the payment, he is assumed to be responsible for the disputed payment until he can show otherwise.

Because the duty to prove facts may affect the protection of the consumer against unauthorised credit card or EFT payments, all the loss allocation schemes discussed in

this study assign the duty to prove the validity of the disputed payment to the issuer. However, the issuer's burden of proof may differ from one loss allocation scheme to another, depending on the rules incorporated in the scheme. From the discussion it appeared that the EFTA and TILA burden of proof rules are more comprehensive than those used in the United Kingdom and the Malaysian loss allocation schemes.

In the United States, for instance, both the TILA and the EFTA require the issuer to show either the payment was initiated by an authorised person, or if not authorised, the consumer had received a benefit from the disputed payment. Under the EFTA, if the issuer cannot prove the validity of the payment based on the agency rule or receipt of benefit rule, it has to show that the payment was fraudulently made by the consumer before it can allocate the losses to the consumer.

Although all the regulations require the issuer to prove the authority of the person who initiated the disputed payment, the standard of proof differs from one jurisdiction to another. In fact, in the United States, different states employ different standards of proof, thereby jeopardising the uniform application of the rule. Unless the rule clearly stipulates the standard of proof required from the issuer, some consumers may enjoy better protection than others if the law in their states imposes a higher standard of proving an agent's authority than the rest of the country. The non-uniformity may be avoided by following the style used in drafting s. 903 (11) of the EFTA, which specifically requires that the fraud which the issuer must prove is fraud with intention to deceive; thus preventing disagreement involving the elements of proving fraud.

Therefore, s 133 and s. 909 of the TILA and the EFTA respectively, should be amended to insert a proviso requiring the issuer to prove the presence of the agency authorities on the balance of probability.

In Malaysia, the EFT Guidelines also require the issuer to prove negligence as a ground of allocating the losses to the consumer. However, the rule failed to specify the elements of negligence which must be proved and also the standard of proof to be discharged by the issuer. Nevertheless, since in Malaysia the standard of proving negligence is certainly on the balance of probability, the flaw in the EFT Guidelines' rule concerning proof of negligence can be remedied by applying the general standard of proving negligence. In fact, applying the general standard of proof would also demand the issuer to show that the losses would not have happened but for the consumer's negligence.

Another aspect of the burden of proof which affects the consumer dearly in the EFT payment systems in Malaysia is the rule in Para 14 of the EFT Guidelines which allow the issuer to prove the proper functioning of the means of accessing the consumer's account and also the EFT system as a conclusive proof of the validity of the disputed EFT payment. This rule is prejudicial to the consumer as it require the consumer to disprove facts which are most of the time beyond his knowledge and comprehension, especially when the risk of fraudulent payment in electronic commerce transactions are not usually understood by the layman. What is more worrying is that the EFT

Guidelines allow the issuer to conceal evidence if the concealment is necessary to protect the security of the issuer or its payment systems.

Apart from proving the validity of the payment or the receipt of benefit or fraud of the consumer, all the regulations also prescribed certain basic underlying conditions which the issuer must prove before it can even think of allocating the losses to the consumer. The most comprehensive regulations in so far as the underlying conditions for the consumer's liability are concerned are the TILA and the EFTA.

One of the conditions incorporated in all the regulations, except the Malaysian CC Guidelines, is that the card or the access code must be an accepted card or code. It is therefore the duty of the issuer to prove that the card and/or code was accepted before it can think of allocating the losses to the consumer. The issuer's failure to discharge this proof destroyed his opportunity to allocate the disputed payment to the consumer.

This duty is beneficial to the consumer, not only in protecting him from losses in the case of a card sent to his address without his knowledge, as in a promotional package, but can also protect the consumer in a situation where his identity is stolen and used to apply for a credit or debit card. This aspect of consumer protection strategy is missing from the Malaysian regime, therefore reducing the level of protection which the consumer should enjoy.

Apart from the above condition, the issuer in the United States must also prove that the consumer was given an identification method that is suitable for the type of commerce system in which the payment will be made. This requirement helps to protect the consumer in circumstances where it is uncertain whether the payment initiated with the use of the card details is covered by the TILA and EFTA loss allocation rules. By having this requirement, the consumer can avoid losses by showing that the payment was initiated in a medium of communication which does not take the identification given by the issuer. Hence, a consumer is protected against losses caused by unauthorised EFT or credit card payment made in a distance transaction where neither the card nor the PIN can be used to identify the person who initiated the payment.

The provision of the identification method is not a character of the loss allocation schemes in the United Kingdom and Malaysia. Therefore, the issuer may still attempt to allocate the losses to the consumer even if the identification it gave to the consumer cannot function to identify the authority of the person who initiated the disputed payment. This approach is against the idea of loss reduction which assigns the losses to the issuer because in the systems where the identification method supplied does not, while the issuer allowed the consumer to transact in those systems, it is best that the issuer innovates and produces a suitable identification method or bears the losses, rather than leaving the consumer to figure out ways to protect himself from the risk of fraud.

The third condition fixed by all the regulations, except the Banking Code and the Malaysian CC Guidelines is the disclosure of the notification method. However, only

the EFTA, the TILA and the CCA use this condition as a precondition for the issuer's right to allocate fraudulent payment losses to the consumer. The Malaysian EFT And CC Guidelines are both silent on the effect of the issuer's failure to inform the consumer of the mode of notification other than that it is an offence under s.57 of the Payment Systems Act 2003. Accordingly, the issuer may still allocate the losses to the consumer, irrespective of the difficulty which the consumer must face before he can take action to prevent or reduce the losses by notification of the events that have facilitated or may facilitate fraudulent payment.

It was shown that in United Kingdom, the Banking Code does not specifically require a disclosure of the notification method. However, it specifically states that the subscribers promise to disclose the consumer's rights and duties in the agreement. Nevertheless, failure of the issuer to disclose does not affect its right to allocate the losses to the consumer unless such a failure constitutes a breach of the implied or express terms of the contract between the issuer and the consumer as when it promised to follow the Banking Code rule. Even if there is such a promise, the Banking Code does not specifically require disclosure of a notification method. Likewise in Malaysia, the issuer of a credit card need not inform the consumer of the way to communicate any unauthorised payment or any potential unauthorised payment.

The lack of such disclosure in these two regulations may affect the consumer's promptness in giving notice of any unauthorised payment to the issuer. Apparently, these two regulations allowed the issuer to specify in its contract terms the time for

notification. Since the notice must be given within the specified time, the consumer's search for information about the notification method, may affect the promptness of the notification, and eventually, his protection against unauthorised payment.

The fourth condition with which the issuer must comply and must prove that it has been complied with is the issuance of a warning of potential liability to the consumer. This disclosure, again like the above disclosure, is intended to educate the consumer about losses which he may have to bear if fraudulent payment occurs and the circumstances when liability attaches to him. Both the EFTA and the TILA prevent the issuer from allocating the losses to the consumer if the issuer failed to prove that the warning has been disclosed to the consumer in the agreement entered into between them. In Malaysia, though the EFT and CC Guidelines required the issuer to issue the same warning, yet they did not prevent the issuer from allocating fraudulent payment losses to the consumer in the event of the issuer failing to satisfy this requirement. The issuer, however, may be charged with an offence under s 57 of the Payment Systems Act 2003 for acting contrary to the Guidelines.

The same requirement is also found in the Consumer Credit (Agreements) Regulations in the United Kingdom. However, this requirement is only imposed on the issuer of a credit card. Accordingly, unless the debit card is used to incur credit, the issuer need not warn the consumer of his liability in the case of an unauthorised payment. The impact of the issuer's failure to disclose a warning is to render the contract unenforceable, thus



preventing the issuer from allocating the losses to the consumer except by the order of the court.

From all the above requirements with which the issuer must comply and must prove that they have been complied with, it is clear that the EFTA and the TILA are the most comprehensive loss allocation rules for the protection of the consumer against any unauthorised payments. These regulations achieved such a higher level of consumer protection by setting a stringent set of conditions which are intended to inform the consumer of action to be taken to avoid, prevent or reduce the losses; imposing on the issuer the duty to prevent or reduce the losses when it is the best party in the circumstances to take suitable action; and also encouraging the consumer to perform certain actions which can prevent or reduce losses.

However, in so far as the burden of proving receipt of benefit is concerned, both the TILA and the EFTA suffer from a lack of a clear standard of proof to be applied in deciding whether the issuer had successfully proven that the consumer had received benefit from the disputed payment or that the payment was fraudulently made by the consumer or by a person with whom he was in cooperation.

In the discussion it was also shown that the burden of proving fraud in Malaysia is uncertain due to differences in opinion of two courts of the same status but with different names. This uncertainty may affect the consumer since the Mediator may choose to follow any of the precedents. If the standard of proving fraud applied by the Mediator is

proof on the balance of probability, the consumer is more easily exposed to losses than if the issuer is required to prove beyond reasonable doubt. Therefore, for purpose of certainty and also to protect the consumer against the effect of using a different standard of proof, the CC Guidelines should be reviewed and amended to expressly stipulate the standard of proof required to show that the payment was fraudulently made by the consumer or a person with whom he is in concert.

Finally, the burden of proving negligence is not mentioned in the United Kingdom Banking Code and the Malaysian EFT Guidelines. However, the standard of proof that is applicable in the civil proceeding should be applied to a dispute involving the allocation of fraudulent payment losses when it is claimed that the payment would not have been made but for the consumer's negligence.

## 1 INTRODUCTION

As previously mentioned, the relationship between the consumer and the issuer is contractual in nature.<sup>1</sup> In this relationship, it is also typical to find the terms to be pre-drafted by the issuer in the standard form contract.<sup>2</sup> Although a contract is not invalid or its term is not unenforceable because it is a standard form contract,<sup>3</sup> there is concern that the contract may be unfair to the consumer. In particular, lack of consumer involvement in the drafting process may give the issuer the opportunity to incorporate clauses that are potentially unfair. These clauses are normally labelled as exclusion clauses, exemption clauses, exculpatory clauses or limitation clauses.<sup>4</sup> Still there are many other contract terms which do not carry this label but may have a similar effect on the consumer as they are used to unfairly allocate the risks of contracting to the consumer.

Generally, a consumer can avoid a contract if it is rendered invalid under any established

---

<sup>1</sup> See Chapter one at 32-37.

<sup>2</sup> Rakoff, T. D., "Contracts of Adhesion: an Essay in Reconstruction" (1983) 96 *Harv. L. Rev.* 1174, at 1190, see at 1222-1225. (Hereafter Rakoff, T. D., "Contracts of Adhesion: an Essay in Reconstruction").

<sup>3</sup> *Rozeboom v Northwestern Bell Telephone Co.*, 358 N.W.2d 241, 47 A. L. R 4th 869 (S. D. 1984). *Carnival Cruise Lines, Inc. v. Shute*, 499 U.S. 585 (1991), Burke, J. J. A., "Contract as Commodity: A Non-fiction Statutory Approach (2000) *Stat Law* 21(12).

<sup>4</sup> *Ailsa Craig Fishing Co. Ltd. v. Malvern Fishing Co. Ltd.*, [1983] 1 Lloyd's Rep. 183, at 389, *per Wilberforce L. J.*, *George Mitchell v Finney Lock Seeds* [1983] Q.B. 284, *Wee Lian Construction Sdn Bhd v Ingersoll-Jati Malaysia Sdn Bhd* [2005] 1 MLJ 162, at 179.

contract rules, legislative or judicial.<sup>5</sup> However, these rules are concerned only with abuse in the contract formation process or procedural fairness but not with substantive fairness. Therefore, in some circumstances, it is necessary for the law to interfere with the contracting parties' choice to contract. In this way, contract terms can be scrutinised so that any term inserted by one party is not enforced against the other if the term is substantially unfair.<sup>6</sup>

Initially, when all elements of a valid contract are present, the enforceability of a contract term is determined by assessing its incorporation into the contract and also by the scope of its coverage. In this assessment, courts apply the incorporation<sup>7</sup> and construction of contract rules.<sup>8</sup> Despite the potential benefit of the rules in excluding terms which the consumer did not know or agree to, they cannot be used to examine the fairness of the terms which were perfectly incorporated and constructed. From this

---

<sup>5</sup> Section 14-19 of the Contract Act 1950, *Williston: A Treatise on the Law of Contracts* § 1:20. Void bargains and voidable contracts.

<sup>6</sup> *Williston: A Treatise on the Law of Contracts*, §18. See Korobkin, R. B., "Bounded Rationality, Standard Form Contracts, and Unconscionability" (2003) 70 *U. Chi. L. Rev.* 1203, for economic arguments to support state intervention in regulating standard form contract. (Hereafter Korobkin, R. B., "Bounded Rationality, Standard Form Contracts, and Unconscionability")

<sup>7</sup> *L'Estrange v F. Graucob Ltd* [1934] 2 K.B. 394, at 402-403, *per* Scrutton L. J, Citing *Parker v. South Eastern Ry. Co.* (1876-77) L.R. 2 C.P.D. 416, at 421 and 428, *per* Mellish, L.J and Bramwell L.J respectively; *Serangoon Garden Estate Ltd v Marian Chye* [1959] MLJ 113; *Rossi v Douglas*, 203 Md. 190, 192, 100 A.2d3, 7 (1953), *Yusof bin Mohamed v Saripah binti Hamzah* [2000] 1 MLJ 827 and *Wee Lian Construction Sdn Bhd v Ingersoll-Jati Malaysia Sdn Bhd* [2005] 1 MLJ 162, at 176 -17.8; *Rossi v Douglas*, 203 Md. 190, 192, 100 A.2d3, 7 (1953), *Bob Wilson, Inc. v Swann*, 168 A.2d 198 (Mun. Ct. App. D.C. 1961)

<sup>8</sup> Malaysian cases, *Lee Yee Yew (Administrator For The Estate Of Lee Teong Lee, Deceased) v United Oriental Assurance Sdn Bhd And Another* [1998] 5 MLJ 763, at 768; United Kingdom cases, *Photo Production Ltd v Securicor Transport Ltd* [1980] A.C. 827, *Dino Services Ltd. v. Prudential Assurance Co. Ltd* [1989] 1 Lloyd's Rep. 379, *Glasgow Training Group (Motor Trade) Ltd v Lombard Continental Plc*, 1989 S. C 30; United States cases *General Motors Acceptance Corp. v. Daniels*, 589 F.2d 761, 767 (4th Cir. 1978), *Brohawn v. Transamerica Ins. Co.*, 276 Md. 396, 347 A.2d 842 (1975), *Gross v. Sweet* 49 NY2d 102, at 107-110, 424 NYS2d 365, 368-370, 400 NE2d 306, 309-311 (1979)

perspective, it is believed that the use of substantively unfair contract terms should be regulated.

In the United States, the enforceability of a contract or its terms is determined by applying the unconscionability of contract rules. These rules were introduced by Art. 2 of the Uniform Commercial Code (the “UCC”) and also s. 208 of the Restatement (Second) of Contract 1981.

In the United Kingdom, the validity of contract terms is determined by applying two different statutory tests; which application, depends on the label given to the contract terms. One of the tests questions the reasonableness of the contract terms. This test was introduced by the Unfair Contract Terms Act 1977 (the “UCTA”). The second test is the fairness test which was introduced by the Unfair Terms in Consumer Contract Regulations 1999 (the “UTCCR”).<sup>9</sup> Apart from that, a credit agreement concluded between the consumer and the card issuer is also governed by the newly inserted s. 140A of the CCA.<sup>10</sup>

Meanwhile, in Malaysia, the validity of the contract terms continues to be assessed, based on the common law rules of incorporation and construction of contract, combined with the Contract Act 1950 which examines the parties’ consent to contract.<sup>11</sup>

---

<sup>9</sup> SI 1999/2083.

<sup>10</sup> Inserted by s 19 of the CCA 2006

<sup>11</sup> See s. 14 – s. 19 of the Contract Act 1950. See *Tan Chin Swee & Anor v Seri Ampangan Realty Sdn Bhd* [2005] 1 CLJ 865, at 872.

To fully understand the regulations of unfair terms and their impact on the protection of the consumer against unauthorised payment, the following discussion will analyse the rules that govern the enforceability of a contract or its terms in the three jurisdictions.

Other than showing the impact of unfair terms on loss allocation the discussion, which analysed several contract terms, will also reveal the impact of the lack of implementation of the EFT and the CC Guidelines on the consumer. In particular, it will show that compared to the position in Malaysia, the issuer of a credit card and debit card in the United States and the credit card issuer in the United Kingdom must strictly comply with the statutory loss allocation rules before any unauthorised payment losses can be allocated to the consumer.<sup>12</sup>

However, the Malaysian position is different. In Malaysia, neither the EFT nor CC Guidelines prohibit contracting out. Regardless of the fact that s. 57 of the Payment Systems Act 2003 makes it an offence for the issuer to contradict the Guidelines, the commission of that offence does not affect the validity and the enforceability of the contract or the contradictory terms. Lack of prohibition on contracting out of the Guidelines' loss allocation schemes harshly affects the consumer when the terms are unfair but satisfies the incorporation and the construction of contract rules.

The discussion continues in section 2 below which focuses on the common law rules

---

<sup>12</sup> Section 133 (e) of the TILA, s. 909(d) of the EFTA and s 173 of the CCA.

of incorporation and construction of contract. Section 3 examines the unconscionable contract rules as used in the United States while Section 4 discusses the unfair terms regulations in the United Kingdom. Section 5 discusses the present state of contract terms regulation in Malaysia while Section 6 analyses some of the terms incorporated in the contract for credit card facility and also the contract for EFT payment via debit card. In this section, the terms reviewed are from the contract used in Malaysia. The terms chosen are those that affect the allocation of fraudulent payment losses and they will be discussed to identify their impact on the consumer from the perspective of the incorporation and construction of contract rules that are applicable in Malaysia, the United States unconscionable contract rules, the UCTA, the UTCCR, and also the CCA rules in the United Kingdom.

## **2 COMMON LAW RULES AND THE ENFORCEABILITY OF CONTRACT TERMS**

### **A Incorporation**

Common law regards contract terms incorporated into a signed contract as binding on the signatories.<sup>13</sup> Therefore, when the consumer signs the contract for electronic

---

<sup>13</sup> *The United States' cases are Rossi v Douglas*, 203 Md. 190, 192, 100 A.2d3, 7 (1953); *Richardson Greenshield Securities Inc. v Metz*, 566 F.Supp. 131 (S.D.N.Y. 1983); the United Kingdom's cases are *L'Estrange v F. Graucob Ltd* [1934] 2 K. B. 394, at 402-403, *per* Scrutton L. J, citing *Parker v. South Eastern Ry. Co.* (1876-77) L.R. 2 C.P.D. 416, at 421 and 428, *per* Mellish, L.J and Bramwell L.J respectively. The Malaysian cases are *Serangoon Garden Estate Ltd v Marian Chye* [1959] MLJ 113, *Yusof bin Mohamed v Saripah binti Hamzah* [2000] 1 MLJ 827 and *Wee Lian Construction Sdn Bhd V Ingersoll-Jati Malaysia Sdn Bhd* [2005] 1 MLJ 162, at 176 -17.8

payment facilities, a credit card or debit card, he is bound by the contract because of his signature. This rule which is based on the consent theory of contract binds the consumer to the signed contract, regardless of whether he read its terms and understood them.<sup>14</sup> Unless it is proven that the consumer was induced to sign the credit agreement or the agreement for the EFT payment facility by any act that defeated his free consent or there is a successful plea of *non est factum*, the consumer cannot avoid the contract.<sup>15</sup> Another ground for avoiding the contract or its terms is for the consumer to show that he was unaware of the terms of the contract or the document he signed was not of a type which could reasonably be expected to contain contract terms.<sup>16</sup>

In the contract for a credit card facility, this is not an issue because the consumer is usually required to sign the credit agreement.<sup>17</sup> Even if the rules which regulate electronic payment systems do not require a signature the presence of the contract terms should be known to the consumer as the credit card and debit card issuers usually incorporate the contract terms into the card application form. Moreover, it is also

---

<sup>14</sup>Ibid. See also Rakoff, T. D., "Contracts of Adhesion: An Essay in Reconstruction" at 1190, and Korobkin, "Bounded Rationality, Standard Form Contracts, and Unconscionability" at 1204.

<sup>15</sup> *Parker v The Southern Eastern Railway Company* (1876-77) L.R. 2 C.P.D. 416, at 421, per Mellish L.J., *Curtis v. Chemical Cleaning and Dyeing Co.* [1951] 1 K.B. 805, at 809, per Denning L.J., *Saunders v Anglia Building Society* [1971] AC 1039, at 1052 per Lord Pearson, *Chin Well Fasteners Co Sdn Bhd v Sampath Kumar Vellingiri & Ors* [2006] 1 MLJ 117, *Subramaniam v Retnam*, [1966] 1 MLJ 172, *Awang bin Omar v Haji Omar bin Ismail & Anor* [1949] MLJ Supp MLJ 28; *Broome Constr. Co. v. Beaver Lake Recreational Ctr., Inc.*, 229 So. 2d 545, 547 (Miss. 1969). See Calamari, J. D. and Perillo, J. M. *The Law of Contracts*, 3<sup>rd</sup> Edn. (1987), s. 9.43, at 414, (Hereafter Calamari and Perillo, *The Law of Contracts*) and Monestier, T. J., "'Nothing Comes of Nothing'. . . Or does It??? A Critical Re-Examination of the Doctrine of Separability in American Arbitration", (2001) 12 *Am. Rev. Int'l Arb.* 223, at 241.

<sup>16</sup> Treitel, G. H., *The Law of Contract*, 10<sup>th</sup> Edn. (1999), at 197, Sweet & Maxwell. (Hereafter, Treitel, G. H., *The Law of Contract*), Knapp, C. L., "A Tribute to Professor Joseph M. Perillo: Taking Contracts Private: The Quiet Revolution In Contract Law" (2002) 71 *Fordham L. Rev.* 761, at 767 and the accompanying note.

<sup>17</sup> See for example s. 61 of the CCA



common for the issuers to refer the consumer to documents which state the terms and conditions for the use of the payment facilities.<sup>18</sup>

## **B Construction**

Assuming that an exclusion clause has been successfully incorporated in the contract for electronic payment facilities, its effectiveness in protecting the issuer against unauthorised payment losses can still be scrutinised by applying the rule of construction.<sup>19</sup>

The construction of contract rule allows courts to ascertain the scope of the contract terms by examining the contract as a whole. Courts will look into the nature of the contract; the type of “contingency or losses that has occurred” and the intention of the parties.<sup>20</sup> Words used in the particular contract terms are also relevant. If the contract term is clearly expressed, courts usually attach to the words used their natural ordinary

---

<sup>18</sup> Treitel, G. H., *The Law of Contract*, at 174-175, 198, *Circle Freight International Ltd v Mideast Gulf Exports* [1988] 2 Lloyd's Rep. 427, *Parker v South Eastern Railway Company* (1876-77) L.R. 2 C.P.D. 416, *Olley v. Marlborough Court Ltd.* [1949] 1 All ER 127 and *McCutcheon v. David MacBrayne Ltd.* [1964] 1 W.L.R. 125; *Malaysian Airlines Bhd v Malini Nathan & Anor* [1986] 1 MLJ 330.

<sup>19</sup> Beale, H. G., *Chitty on Contracts*, at paras 14-005 – 14-024, at 793-810, Treitel, G. H., *The Law of Contract*, at 201-221, Farnsworths, *Contracts*, Chp 7, especially ss.7.7-7.14.; McBryde, W. W., *The Law of Contract in Scotland*, 2<sup>nd</sup> Edn, (2001), Chp 8, W. Green, (Hereafter, McBryde, W. W., *The Law of Contract in Scotland*), s. 203 of the Restatement of Second of Contract and *Williston: A Treatise on the Law of Contract*, § 30, Interpretation and Construction of Contract.

<sup>20</sup> Beale, H. G., *Chitty on Contract*, at para 14-005. *Siong Electronic Industries* (1981) *Sdn Bhd v Sanyo Sales & Service Sdn Bhd* [1997] 162 MLJU 1, at 6, *Ayer Hitam Tin Dredging Malaysia Bhd v YC Chin Enterprises Sdn Bhd* (1994) 2 MLJ 754, at 764; United Kingdom case *Vitol BV v Compagnie Europeene des Petroles* [1988] 1 Lloyd's Rep 574 at p 576, *Reardon-Smith Line Ltd. v Hansen-Tangen* (1976) 1 W.L.R. 125), *Equity & Law Life Assurance Society plc v Bodfield Ltd* (1987) 281 E.G 1448 and *Association of British Travel Agents Ltd. and Others v. British Airways Plc and Others* [2000] 2 Lloyd's Rep. 209, 216 and 218., United States case *Wilke v. First Federal Sav. and Loan Ass'n of Eau Claire* 108 Wis.2d 650, 323 N.W.2d 179 Wis.App., 1982, *Strategic Staff Management, Inc. v. Roseland* 260 Neb. 682, 619 N.W.2d 230 Neb., 2000.

meaning.<sup>21</sup> However, where it finds the language ambiguous,<sup>22</sup> courts will construct the contract based on the *contra proferentum*<sup>23</sup> rule whereby the clause is interpreted against the issuer's interest.<sup>24</sup>

In case a contract term purports to protect the issuer from the effect of its own negligent conduct which injures the consumer, the courts will be more rigorous in interpreting the words used.<sup>25</sup> Hence, for the issuer to use its contract term to effectively exclude itself from being liable for its own negligence, the words used in the term must clearly point out that intention. Thus, words like "negligence" or other words that are wide enough to be understood to include negligence such as "sole risk" or "no liability whatever" are more effective in excluding the issuer from fraudulent payment caused by its own negligence.<sup>26</sup>

---

<sup>21</sup> *General Motors Acceptance Corp. v. Daniels*, 589 F.2d 761, 767 (4th Cir. 1978), *Brohawn v. Transamerica Ins. Co.*, 276 Md. 396, 347 A.2d 842 (1975), *Photo Production Ltd v Securicor Transport Ltd* [1980] A.C. 827, *Dino Services Ltd. v. Prudential Assurance Co. Ltd* [1989] 1 Lloyd's Rep. 379, *Glasgow Training Group (Motor Trade) Ltd v Lombard Continental Plc*, 1989 S. C. 30, *Jerneh Insurance Corp Sdn Bhd v Amanah Raya Bhd* [1998] 7 MLJ 115, *Persin Kaur v The Renong Tin Dredging Co Ltd* [1967] 2 MLJ 286, *Syarikat Uniweld Trading v The Asia Insurance Co Ltd* [1996] 2 MLJ 160 and *Malaysia National Insurance Sdn Bhd v Abdul Aziz bin Mohamed Daud* [1979] 2 MLJ 29.

<sup>22</sup> See details discussion on ambiguous contract terms in Lewison, K., *The Interpretation of Contracts*, 3<sup>rd</sup> Edn. (2004), Chp 7, Sweet & Maxwell.

<sup>23</sup> *Ibid*, Chp 6, para 6.07, at 168-174 for a discussion on the *contra proferentum* rule. See also Beale, H. G., *Chitty on Contracts*, para 14-14-009, at 797-798, and *Williston: A Treatise on the Law of Contract*, §32.12 *Contra proferentem: Ambiguities interpreted against drafter*.

<sup>24</sup> Treitel, G. H., *The Law of Contract*, at 200-201, Farnsworth, *Contracts* at para 7.13, at 471-472, McBryde, W. W., *The Law of Contract in Scotland*, para 7.23- 7.34, at 170-174, *J. Spurling Ltd v Bradshaw* [1956] 1 W. L. R 461, *McCutcheon v David MacBrayne Ltd* [1964] 1 W. L. R. 125, *Foreswood Timber SB v Rajang Line SB & Ors* [1999] 159 MLJU 1, *M.J. Bradley Company, Inc. v. General Polymers Corp States* 1994 U.S. Dist. LEXIS 15489.

<sup>25</sup> Beale, H. G., *Chitty on Contract*, para 14-010, at 498,

<sup>26</sup> *Ibid*, para 14-010-14-013, at 800-802. See also Lawson R. G., *Exclusion Clause and Unfair Contract Terms*, 7<sup>th</sup> Edn (2003) Sweet & Maxwell, McBryde, W. W., *The Law of Contract in Scotland*, chp 8, and *Williston: A Treatise on the Law of Contract*, chp 18. *Canada Steamship Lines Ltd v R* [1952] 1 All ER 305, *Smith v UMB Chrysler (Scotland) Ltd* 1978 SC (HL) 1, *Premier Hotel Sdn Bhd v Tang Ling Seng* [1995] 4 MLJ 229, *Kuok Ling Timber Industries Sdn Bhd v The Owners of and Other Persons Interested in the Vessel "Mv Thonfullin"* [2000] 2 MLJ 615. See Rosenkranz, E. J., "The Pollution Exclusion Clause

Both the incorporation and construction of contract rules are concerned with the formation of the contract.<sup>27</sup> Therefore, where the contract or its terms conform to these two rules, the consumer is bound to contract terms which allocate fraudulent payment losses unfairly. For example, the contract terms may allocate the losses to the consumer for his failure to act or to abstain from certain acts.

The issuer who inserted the terms may not at all be concerned with the consumer's inability to conform to the contractual requirement. In particular, the issuer may not consider the effect of the consumer's lack of knowledge about the contractual requirement, technical complexity of the requirement and also financial weaknesses as relevant to successful performance of the contractual requirement.

From an economic perspective, the term which allocates the losses to the consumer without regard to his ability to take action to prevent or reduce losses, is inefficient.<sup>28</sup> In terms of justice, the clause may affect fair dealing between the parties. Therefore, unless the contract between the consumer and the issuer failed the incorporation or the construction rules or other rules that are concerned with free consent, the consumer will be responsible for unauthorised payment losses as a result of the use of unfair terms. In view of that, legislative intervention is necessary.

---

Through the Looking Glass", (1986) 74 *Geo. L.J.* 1237, for the different construction of an exclusion clause that purport to exclude liability for negligence in various different states in the United States of America.

<sup>27</sup> Cranston, R., *Principles of Banking Law* 2<sup>nd</sup> Edn (2002), at 160, Oxford University Press.

<sup>28</sup> This is known as a failure to take precaution to prevent or reduce losses from unauthorised payment. See Cooter, R. D. and Rubin, E.L., "A Theory of Loss Allocation for Consumer Payments", at 73-77.

### 3 LEGISLATIVE INTERVENTION IN THE UNITED STATES

The contract between the consumer and the issuer of electronic payment facilities is usually in the form of a standard form contract.<sup>29</sup> This contract satisfies the criteria of a contract of adhesion, namely, it was prepared by the issuer for the consumer on a “take it or leave it basis”;<sup>30</sup> the issuer is in a superior bargaining position compared to the consumer<sup>31</sup>; and the consumer may be oppressed by harsh terms due to a lack of negotiation.<sup>32</sup>

In *Comb v PayPal*<sup>33</sup> and *Hutcherson v. Sears Roebuck & Co.*<sup>34</sup> the courts explained that a contract which has the above characteristics deprives the consumer who wishes to acquire the service of any other choices other than to accept the terms in full.

A standard form contract is undeniably economical since the consumer does not have to spend time and expenses on negotiating for favourable terms.<sup>35</sup> He can choose the best

---

<sup>29</sup> The contract is also known as an “adaptable contract” because it contained some regulatory prescribed terms and some negotiable terms. See Geva, B., “Forged Check Indorsement Losses under the UCC: The Role of Policy in the Emergence of Law Merchant from Common Law”, (2000) 45 *Wayne L. Rev.* 1733.

<sup>30</sup> Stempel, J. W., “A Better Approach to Arbitrability,” (1991).65 *Tul. L. Rev.* 1377, at 1431.

<sup>31</sup> *Neal v. State Farm Ins. Cos.* 10 Cal. Rptr. 781 (Cal. Dist. Ct. App. 1961) at 784. *per* Justice Mathew O. Tobriner.

<sup>32</sup> In *Graham v Scissor-Tail, Inc.* 623 P.2d at 171 (Cal., 1981) the court said, “It is in the context of this tension--between social advantage in the light of modern conditions on the one hand, and the danger of oppression on the other--that courts and legislatures have sometimes acted to prevent perceived abuses”.

<sup>33</sup> 218 F.Supp.2d 1165 (N.D. Cal. 2002). See Rakoff, T. D., “Contracts of Adhesion: an Essay in Reconstruction” at 1177-1178.

<sup>34</sup> 342 Ill.App.3d 109, 276 Ill.Dec. 127 Ill.App. 1 Dist.,2003. See earlier case such as *Carpenter v Suffolk Franklin Sav. Bank* 370 Mass. 314, 346 N.E.2d 892 Mass. 1976 and *Anderson v. Baker* 196 Mont. 494, at 501, 641 P.2d 1035, at 1039, Mont., 1982.

<sup>35</sup> The benefits may include reducing the transaction cost and simplify the business operations, increasing the drafter experience with the “interpretation of similar forms” and also “make risk calculable.” See

terms of all the issuers' contract terms available in the market. However, "conscious parallelism" among the issuers may create an identical standard form contract which leaves the consumer with little or no choice of a better deal at all.<sup>36</sup> For example, when most contracts for long-distance telephone facilities offered by different suppliers in the market contain arbitration clauses it was held that the consumer was deprived of "any meaningful choice".<sup>37</sup> The lack of opportunity to choose the best contract terms can also be found in contracts involving electronic payment systems, credit or debit cards, because almost all contract terms found in the market are identical.

Despite the above comment, a contract of adhesion is not in itself unenforceable.<sup>38</sup> To avoid this contract or its terms, the consumer has to rely on the same rules that are applicable to a negotiable contract.<sup>39</sup> However, since the rules, as mentioned earlier, cannot prevent the use of contract terms on the grounds of substantive fairness, it is necessary to have rules that protect the consumer against unfair terms, substantively and procedurally. In this regard, the unconscionability of contract rules provides the

---

Farnsworth, *Contracts*, s. 4.26, at 286, and Rakoff, T. D., "Contracts Of Adhesion: An Essay In Reconstruction" at 1220- 1225.

<sup>36</sup> *Germantown Mfg. Co. v. Rawlinson* 491 A.2d 138, 147 (Pa. Super. 1985). See contrary decision in *Ranieri v Bell Atlantic Mobile*, 304 AD2d 353, 354 [1st Dept 2003] "[i]t does not avail plaintiff to argue that the arbitration provision is unconscionable without offering evidence that he could not have chosen another service provider".

<sup>37</sup> *Ting v. AT&T* 182 F.Supp.2d 902 N.D.Cal.,2002.

<sup>38</sup> *Broemmer v. Abortion Services of Phoenix, Ltd.*, 173 Ariz. 148, at 151, 840 P.2d 1013, 1016 Ariz.1992), and *Graham v. Scissor-Tail, Inc.*, 28 Cal.3d 807, 171 Cal.Rptr. 604, 611, 623 P.2d 165, 172 (1981).

<sup>39</sup> See also *Graham v. Scissor-Tail, Inc.*, 28 Cal. 3d 807, 820 171 Cal. Rptr. 604, 611, 623 P.2d 165, 172 (1981), Spanogle, J. A. Jr., "Analyzing Unconscionability Problems" (1969) *Pennsylvania Law Review*, Vol. 117 No. 7, 931, at 934. (Hereafter Spanogle, J.A., "Analyzing Unconscionability Problems").

necessary basis for challenging both the procedural and the substantive fairness of the contract terms.<sup>40</sup>

## **A Procedural Unconscionability**

A contract or its term is unconscionable because of the defect in the formation process. This defect can be caused by many events that constitute unfair surprise. For example, one of the contracting parties, usually the merchant, may use deceptive methods such as complex wording, phrases and clauses, which are barely understood by the consumer, and also to put clauses into the fine print.<sup>41</sup>

The above actions affect the validity of a contract term because they violate the reasonable expectation of the consumer in the sense that he was not made aware of their presence in the contract.<sup>42</sup> For example, in the case of *Smith v. Idaho State University Federal Credit Union*,<sup>43</sup> the court found the contract to be procedurally unfair because the wife did not know about the terms that bound her to the liability of her husband when he pledged their joint-asset, deposited with the respondent, as collateral to his debt.

---

<sup>40</sup> *Discover Bank v. Superior Court* 36 Cal.4th 148, 30 Cal.Rptr.3d 76 Cal.,2005, and *Szetela v. Discover Bank* (2002) 97 Cal.App.4th 1094, 118 Cal.Rptr.2d 862. *Smith v. Mitsubishi Motors Credit of America, Inc.*, 247 Conn. 342, 721 A.2d 1187 (1998), and *Andersons, Inc. v. Horton Farms, Inc.*, 166 F.3d 308, 1998 FED App. 368P (6th Cir. 1998).

<sup>41</sup> Spanogle, J.A., "Analyzing Unconscionability Problems", at 943. See *Zapatha v. Dairy Mart, Inc.* 381 Mass. 284, 408 N.E.2d 1370 Mass., 1980.

<sup>42</sup> *Ibid*, at 947-948, 954 and 963-964.

<sup>43</sup> 114 Idaho 680, 686, 760 P.2d 19 (1988).

Procedural abuse may also occur as a result of oppression because the merchant uses terms that are unreasonable or that would impair the core terms of the contract.<sup>44</sup> For instance, in the case of *A & M Produce Co. v FMC Corporation*,<sup>45</sup> a disclaimer for warranty of the basic performance of the machinery sold by the seller to the buyer was held to be unreasonable because product performance was a fundamental basis for the contract entered into between the parties.

It should be noted that the adhesion contracts that are usually examined for unconscionability are the contracts between the consumer and his bank in relation to the supply of banking services including payment facilities.<sup>46</sup>

## **B Substantive Unconscionability**

Substantive unconscionability concerned with the effect of the contract on the parties. The effect of this contract is examined by looking at the unfairness of the substance of the contract. The use of harsh, oppressive or one-sided terms are among the indicators of unfair substance.<sup>47</sup> Factors that are taken into consideration in judging the substantive unconscionability of contract terms include “the commercial reasonableness of the

---

<sup>44</sup> Ibid, at 956-962.

<sup>45</sup> 135 Cal.App.3d 47, 492, 186 Cal.Rptr. 114 Cal.App.,1982.

<sup>46</sup> *Comb v PayPal* 218 F.Supp.2d 1165 (N.D. Cal. 2002). and *Hutcherson v. Sears Roebuck & Co.* 342 Ill.App.3d 109, 276 Ill.Dec. 127 Ill.App. 1 Dist.,2003, *Carpenter v Suffolk Franklin Sav. Bank* 370 Mass. 314, 346 N.E.2d 892 Mass. 1976, *Anderson v. Baker* 196 Mont. 494, at 501, 641 P.2d 1035, at 1039, Mont., 1982, *Szetela v. Discover Bank* 97 Cal.App.4th 1094, 1100, 118 Cal.Rptr.2d 862 (2002), and *Strand v US National Bank* 693 N.W.2d 918N.D.,2005.

<sup>47</sup> See *Williston: A Treatise on the Law of Contract*, §18.10 and Leff, A. A., “Unconscionability and the Code--The Emperor's New Clause”, (1967) 115 *U. Pa. L. Rev.* 485, at 509.



contract terms, the allocation of risks between the parties, and also public policy concerns.”<sup>48</sup> The commercial setting of the contract; whether it is a consumer contract or a contract between businesses, and the terms of the contract including their purpose and effect are also relevant to determine the fairness of the contract from the substantive perspective.<sup>49</sup>

Suppose that a contract between the consumer and the issuer contained a clause which would allow the issuer to treat all payment initiated through the electronic systems by using the consumer’s access code as authorised payment. This clause would indirectly allocate to the consumer any unauthorised payment caused by unauthorised access to his electronic payment facility despite the fact that the security breach that facilitated the unauthorised access would have occurred without his knowledge.<sup>50</sup> Regardless of the consumer’s consent to the term, if the term is scrutinised by taking into account the nature of the contract for payment facilities; where the issuer is basically authorised to make payment only upon receiving the consumer’s mandate, the internet security risk, and also the adhesive nature of the contract, the term looks unfair and therefore, unconscionable.

Once the contract or its terms are found to be unconscionable, the courts may refuse to -

---

<sup>48</sup> *NEC Techs., Inc. v. Nelson*, 267 Ga. at 392, 478 S.E.2d at 772.

<sup>49</sup> Section 2-302(2) of the UCC and s. 208 comment f of the Restatement (Second) of Contract 1981. *Williston: A Treatise on the Law of Contract*, at §18.10. See also *Maxwell v. Fidelity Financial Services, Inc.*, 184 Ariz. 82, 907 P.2d 51, 28 U.C.C. Rep. Serv. 2d 806 (1995). In *NEC Techs., Inc. v. Nelson*, 267 Ga. 390, 478 S.E.2d 769, 771 (1996) the court said that substantive unconscionability requires an examination of the contractual terms themselves.

<sup>50</sup> See Chapter Introduction at 2-3.



enforce the contract as a whole or any of its terms.<sup>51</sup> It should be noted that in both s. 2-302 of the UCC and s. 208 of the Restatement (Second) of Contract 1981, the time at which unconscionability is to be determined is when the contract was concluded.<sup>52</sup>

Based on the discussion, it is clear that in the United States, the enforceability of a contract or its terms can be challenged by showing that the contract suffered from procedural and substantive abuse. In fact, it was said that when a contract is an adhesion contract, the courts can straight away examine the substantive unconscionability of the disputed term without looking into procedural unconscionability.<sup>53</sup>

#### **4 LEGISLATIVE INTERVENTION IN THE UNITED KINGDOM**

##### **A Unfair Contract Terms Act 1977**

In the United Kingdom, the courts' authority to supervise the enforceability of contract terms was improved when the UCTA came into force in 1977. The UCTA empowers the courts to examine the enforceability of contract terms beyond the formation process.

---

<sup>51</sup> Comment g s. 208 of Restatement (Second) of Contracts 1981 provides that if the whole contract is unconscionable the remedies include denial of specific performance, denial of money damages and if only a term is or terms are unconscionable, the appropriate remedy is to deny the effect to the unconscionable term. See also Section 2.302(1) of the UCC.

<sup>52</sup> Section 2.302(1) UCC and s. 208 Restatement (Second) of Contracts 1981. *Williston: A Treatise on the Law of Contracts*, §18.12.

<sup>53</sup> Section 208 comment a of the Restatement (Second) of Contracts 1981. The same application of the rule applies to s. 2-302 of the UCC. See *Williston: A Treatise on the Law of Contract*, §18.3, and *Jones v Star Credit Corp.* 59 Misc.2d 189, 298 N.Y.S.2d 264 N.Y.Sup. 1969.

It allows the courts to look into the reasonableness of the substance of the contract.<sup>54</sup> With this authority, the courts can scrutinise the reasonableness of the contract entered into between the consumer and the issuer as the UCTA clearly provides that it is to be used to regulate a contract between the consumer and another party who contracted “in the course of business”.<sup>55</sup>

The UCTA is applicable to a dispute involving terms in a negotiated contract and also in a standard form contract.<sup>56</sup> Despite its wide coverage, the courts can only use the UCTA reasonableness test to examine the use of an exclusion clause.<sup>57</sup> Although the UCTA’s narrow scope of application may limit its effectiveness, its description of an exclusion clause is rather wider than understood in common law. In fact, the UCTA looks into the substance of the clause rather than the label. Hence, the issuer may call the clause by any name yet it is still an exclusion clause under the UCTA if the purpose is to:

- (a) exclude or limit the issuer’s liability for its own breach of contract;<sup>58</sup>
- (b) alter the issuer’s contractual obligation so that it changes what the consumer would reasonably expect to receive from the issuer;<sup>59</sup>

---

<sup>54</sup> *Cremdean Properties Ltd v Nash* [1977] 244 E. G. 547, at 51, *Philips Products Ltd v Hyland* [1987] 1 W. L. R. 659, at 666, *Johnstone v Bloomsbury H. A.* [1992] Q. B. 333, at 346, and *Director General of Fair Trading v First National Bank* [2002] 1 Lloyd’s Rep. 489, para 17.

<sup>55</sup> Section 12(1) and s. 17(2) UCTA. See *Stevenson v Rogers* [1999] 1 All ER 613, at 626.

<sup>56</sup> *Supra* n 54.

<sup>57</sup> Sections 3, 4, 17, 18 11(2) and 24(2) of the UCTA.

<sup>58</sup> Section 3(2)(a) and s. 17(1)(a) UCTA. Beale, H. G., *Chitty on Contracts*, para 14-073 and the Law Commission and the Scottish Law Commission, “Unfair Terms in Contracts” Cm 6464 February 2005, at 9 (the “Report”). See *Charlotte Thirty Ltd v Crocker Ltd* [1990] 24 Const. L. R. 46.

<sup>59</sup> Section 3(2)(b)(i) and s. 17(1)(b) UCTA. See *Zockoll Group Ltd v Mercury Communication Ltd* (No.2) [1998] 1 T. C. L. T 104, *Shearson Lehman Hutton Inc. v MacLaine Watson & Co. Ltd.* [1989] 2 Lloyd’s Rep. 570, at 612 and *SAM Business System Ltd v Hedley & Co.* [2003] 1 All E. R. (Comm) 465.

- (c) alter the issuer's contractual bargain in such a way that it need not perform his bargain in part or in total;<sup>60</sup>
- (d) transfer the issuer's risk of contracting to the consumer via indemnification;<sup>61</sup> and
- (e) exclude or limit the issuer's liability for its negligence action in the performance of its contractual obligation.<sup>62</sup>

The scope of an exclusion clause under the UCTA<sup>63</sup> also covers clauses that impose on the consumer restrictive or onerous conditions<sup>64</sup> and clauses that restrict or limit the consumer's right or remedy in respect of the issuer's liability.<sup>65</sup> Clauses that exclude or limit the rule of evidence or procedures may also fail the UCTA's reasonableness test. Hence, a clause that limits the consumer's mode of settling a dispute to arbitration, when arbitration is not required by legislation and is unaffordable by the consumer, is unenforceable on ground of unreasonableness.<sup>66</sup>

In assessing the reasonableness of any term contained in an exclusion clause, the courts have to consider whether the consumer and the issuer reasonably expect the term to be part of their contract.<sup>67</sup> This expectation is to be searched through all the circumstances

---

<sup>60</sup> Section 3(2)(b)(ii) and s. 17(1)(b) UCTA.

<sup>61</sup> Section 4 and s. 18 UCTA.

<sup>62</sup> Section 2 read together with s. 1 (1)(a)(b) UCTA.

<sup>63</sup> Section 13 and 25 of the UCTA.

<sup>64</sup> *Gransville Oil & Chemical Ltd* [2003] 2 Lloyd's Rep 350, and *BHP Petroleum Ltd v British Steel Plc* [1999] 2 Lloyd's Rep. 586, at 592.

<sup>65</sup> *Stewart Gill Ltd v Horatio Myer & Co.* [1992] Q. B. 600 and *Esso Petroleum Co. Ltd. v Milton* [1997] 1 W. L. R. 938.

<sup>66</sup> *Howard Marine & Dredging Co. Ltd v A. Ogden & Sons (Excavations) Ltd* [1978] Q. B. 574.

<sup>67</sup> Section 11(1) UCTA and s. 24 (1) UCTA. See Steyn, J., "Fulfilling the Reasonable Expectations of Honest Man", (1997) 113 *LQR* 433 (Hereafter Steyn, J., "Fulfilling the Reasonable Expectations of Honest Man") and *Schenkers Ltd. v. Overland Shoes Ltd* [1998] 1 Lloyd's Rep. 498.

surrounding the contract at the time of its conclusion.<sup>68</sup> In *First Energy (UK) Ltd v. Hungarian International Bank Ltd*,<sup>69</sup> for instance, it was held that the relevant circumstances are those that were common between the parties, including the parties' knowledge of the kind of transaction they are involved in and the pre-contractual negotiation which they have had before the contract was concluded.<sup>70</sup>

In some cases where the dispute is concerned with restricting the issuer's liability to a specific amount of money, a determinable sum of money,<sup>71</sup> the courts may take into account the issuer's capacity to bear the cost and to insure against the risk.<sup>72</sup> The courts will also examine the law and public policy that are in place in order to determine the parties' reasonable expectation.<sup>73</sup> Therefore, in case of the electronic payment systems, it is necessary for the courts to examine the relevant regulations including the CCA, the Banking Code and also the general law of banking which govern the relationship between the consumer and the issuer.

---

<sup>68</sup> Section 11(1) UCTA and s. 24 (1) UCTA.

<sup>69</sup> [1993] 2 Lloyd's Rep. 194, at, 200-201 *per* Steyn L. J.

<sup>70</sup> Beale, H. G., *Chitty on Contracts*, para 14-084 and Steyn, J "Fulfilling the Reasonable Expectations of Honest Man", at 433-434. See *SAM Business Systems Ltd v Hedley & Co.* [2003] 1 All ER (Comm) 465 and *Bank of Scotland v. Dunedin Property Investment Co Ltd* 1999 S.L.T. 47.

<sup>71</sup> Beale, H. G., *Chitty on Contracts*, para 14-087.

<sup>72</sup> This rule corresponds to the loss spreading principle discussed in Cooter, R. D. and Rubin, E. L., "A Theory of Loss Allocation for Consumer Payments". See *Singer Co. (U.K.) Ltd. v. Tees and Hartlepool Port Authority* [1988] 2 Lloyd's Rep. 164 and *Flamar Interocean v Denmac (The Flamar Pride and The Flamar Progress)* [1990] 1 Lloyd's Rep. 434 and *Monarch Airlines Ltd v London Luton Airport* [1998] 1 Lloyd's Rep. 403,

<sup>73</sup> Steyn, J., "Fulfilling the Reasonable Expectations of Honest Man", and *British Airports Authority plc v. British Airways Board* [1981] S. & B. AvR. 111/29, at 34 where Parker J. remarked that when the clause was allowed by the law it is not against public policy hence reasonable. Quoted in *Monarch Airlines Ltd. v. London Luton Airport Ltd.* [1998] 1 Lloyd's Rep. 403, at 406.

To test the reasonableness of the respective contract term the courts must analyse the whole clause in which the term is contained, and if the contract contains sub-clauses, all the sub-clauses should be considered in their entirety for reasonableness.<sup>74</sup> Therefore, if one of the sub-clauses affects the reasonableness of the whole clause, the whole clause becomes unreasonable.

Apart from the discretionary concept of reasonableness, the guidelines given in Schedule 2 of the UCTA which are concerned with the transfer of ownership or possession in goods can also be used by analogy to analyse the reasonableness of the terms in a contract for electronic payment facilities.<sup>75</sup> For instance, if a disputed term in a contract for credit card facility falls under any of the listed circumstances that indicate unreasonableness, the courts may hold the term unreasonable. In *Schenkers Ltd. v. Overland Shoes Ltd.*,<sup>76</sup> a case involving a contract for transportation, Pill L. J. applied the guidelines in Schedule 2 and found the disputed contract terms reasonable because the parties were of equal bargaining position; the plaintiff's consent was freely given and, based on previous dealings, the parties knew about the disputed terms at the time of contracting.<sup>77</sup>

---

<sup>74</sup> *Stewart Gill Ltd v Horatio Myer & Co. Ltd* [1992] QB 600 and also *AEG (UK) Ltd v Logic Resource Ltd* [1995]

<sup>75</sup> Section 11(2), s. 24(2), s. 6, and s. 7 of the UCTA. See Treitel, G. H., *The Law of Contract*, at 238, and Beale, H. G., *Chitty on Contracts*, para 14-085.

<sup>76</sup> [1998] 1 Lloyd's Rep. 498, at 505 – 508. The court in this case approved the decision in *Stewart Gill Ltd. v. Horatio Myer and Co. Ltd.* 1992] Q.B. 600, at 608 *per* Stuart-Smith L. J.

<sup>77</sup> See also *McCullagh v. Lane Fox & Partners Ltd* [1996] 1 E.G.L.R. 35.

The factors relied on by the courts in finding unreasonableness in the cases discussed earlier are not conclusive evidence of unreasonableness. They only provide general guidelines of the elements that are relevant in assessing the reasonableness of contract terms. The finding of reasonableness or unreasonableness of the terms depends on the facts of each individual case.

Apparently, the consumer's contract with the issuer can now be concluded electronically by virtue of the changes made by the Consumer Credit Act 1974 (Electronic Communications) Order 2004 (the "Order").<sup>78</sup> Despite the changes, the UCTA reasonableness test can still be applied to challenge the validity of an exclusion clause as the requirement of a written contract in s.3 (1) of the UCTA only applies to a contract between businesses.<sup>79</sup>

A similar observation can also be made about an electronic contract for EFT payment facilities as a written agreement is not a requirement, neither in the general law of banking nor in the Banking Code.<sup>80</sup> Hence, a consumer may contest the validity of an electronically concluded EFT contract or its terms on the grounds of unreasonableness under s. 3(1) of the UCTA.

---

<sup>78</sup> SI 2004/3236.

<sup>79</sup> *Flamar Interocean Ltd. v. Denmac Ltd. (Formerly Denholm Maclay Co. Ltd), (The 'Flamar Pride' and 'Flamar Progress')* [1990] 1 Lloyd's Rep. 434 QBD (Comm Ct), at 438.

<sup>80</sup> Section 6 (2) of the Code provides that terms and conditions in relation to a contract for the services stated in s.1 (1) is to be given to the consumer in writing. However, s. 7(1) which dealt with cooling off period mentioned about the possibility of the terms and conditions to be given to the consumer in an electronic forms.

Furthermore, even if the requirement of writing applies to a contract between the consumer and the issuer of a credit or debit card, the definition of writing in Schedule 1 of the Interpretation Act 1978 which “includes typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form...” indicates that electronic contract is also a written contract if the document is visible.<sup>81</sup> Hence, an electronically concluded contract or its terms may also be subjected to the UCTA’s reasonableness test.

## **B      Unfair Terms in Consumer Contract Regulations 1999 (the “UTCCR”)**

Like the UCTA, the UTCCR<sup>82</sup> is intended to regulate the substance of a contract apart from the process of its formation.<sup>83</sup> However, compared to the UCTA, the UTCCR applies the test of fairness to assess the enforceability of only non-negotiated terms in a consumer contract, irrespective of the label of the clause in which the terms are incorporated.<sup>84</sup> Accordingly, any clause, exclusion or not, can be examined by applying the UTCCR rules. However, any term that is concerned with the definition of the subject matter of the contract or the adequacy of the price (the core terms) cannot be

---

<sup>81</sup> The Law Commission, “Electronic Commerce: Formal Requirements In Commercial Transactions” December 2001, Part 3, at 7-16, at <<http://www.lawcom.gov.uk/docs/e-commerce.pdf>> (Visited 12<sup>th</sup> July 2005).

<sup>82</sup> SI 1999/2083

<sup>83</sup> UTCCR was passed to implement the EU Directive on Unfair Terms in Consumer Contracts, OJ L 095 of 21.4. 1993, at 29. See also the EU Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). OJL 178/1. Article 8 of the Directive, for instance, requires member states to facilitate the formation of contract by electronic means, while article 9-11 concern with formation of contract through electronic means. See the United Kingdom Electronic Communications Act 2000, which broad aim is to facilitate e-commerce.

<sup>84</sup> See Reg. 4 (1)Reg. 3(1) and Reg. 5 of the UTCCR



subjected to the fairness test<sup>85</sup> except when they are not “in plain, intelligible language”.<sup>86</sup> Furthermore, the fairness test cannot be used to challenge the enforceability of contract terms inserted to fulfil a legislative requirement.<sup>87</sup>

The UTCCR is not concerned with the form of the contract. Therefore, its fairness test can be used to examine the terms of a standard form contract and also the terms of a negotiated contract when the disputed term was not individually negotiated. Under the UTCCR, a negotiation does not pay lip service but is about genuine negotiation where the consumer is able to influence the substance of the disputed term.<sup>88</sup>

In the case of a term that purports to protect the issuer from its own negligence, the UTCCR allows the courts to examine its fairness to decide its enforceability. This rule differs from the UCTA’s approach, which totally invalidates any term that purports to protect the issuer against its own negligence.<sup>89</sup>

The UTCCR fairness test as described in Reg. 5(1) consists of three components that complement each other, namely; good faith, the term does not cause a significant imbalance in the parties’ rights and obligation, and the imbalance should not be to the

---

<sup>85</sup> Regulation 6(2) (a)(b) UTCCR.

<sup>86</sup> The Core terms must be in a written form to be subjected to the “plain intelligible test”. See Reg. 7(1) UTCCR See *Bankers Insurance Co. Ltd v South* [2003] EWHC 380 (QB).

<sup>87</sup> Regulation 4(2) (a). See Steyn, J., “Fulfilling The Reasonable Expectations Of Honest Man” at 434 where his Lordship accepted that looking for the contractual parties’ expectation in order to find the fairness of a contract, the court has to take into account the law and the public policy.

<sup>88</sup> Reg. 5(2) UTCCR.

<sup>89</sup> Section 2(1) of the UCTA.



detriment of the consumer.<sup>90</sup> Therefore, the first step to be taken is to determine whether the contract terms caused a significant imbalance in the parties' rights and obligations.<sup>91</sup> In this process the courts are guided by the second component of the test, i.e., the good faith principle of fair and open dealing.<sup>92</sup> If the term is found to be unfair the term is rendered invalid only if that unfairness is caused to the consumer.

In considering the fairness of a contract term under the UTCCR, the courts must take into account the circumstances surrounding the contract at the time of its conclusion<sup>93</sup> including the language used in the contract,<sup>94</sup> the clarity and eligibility of the terms,<sup>95</sup> the parties' bargaining position, and the consumer's lack of choice.<sup>96</sup> In *Director General of Fair Trading v First National Bank*,<sup>97</sup> Lord Justice Bingham said that these elements would reveal the fairness of the contract from two perspectives namely, procedural and substantive fairness.

Apart from that, the nature of the contract and its purpose are also relevant.<sup>98</sup> Hence, in

---

<sup>90</sup> *Director General of Fair Trading v First National Bank* [2002] 1 Lloyd's Rep. 489.

<sup>91</sup> Beale, H. G., *Chitty on Contracts*, para 15-049.

<sup>92</sup> *Director General of Fair Trading v First National Bank* [2002] 1 Lloyd's Rep. 489, para 17 *per* Bingham L. J., *Interfoto Picture Library Ltd. v Stiletto Visual Programmes Ltd.* [1988] 1 All ER 348, and Beale, H. G., *Chitty on Contracts*, para 15-049. See also the opinion of the OFT in the Office of Fair Trading Bulletin, "Unfair Contract Terms Guidance", at 3 (2001) at <<http://www.offt.gov.uk/NR/rdonlyres/4A14F0DB-F0A7-4EBB-B68F-F2E9D1A25EF7/0/oft311intro.pdf>> (Visited 10<sup>th</sup> April 2006).

<sup>93</sup> Regulation 6(1) UTCCR. Beale, H. G., *Chitty on Contracts*, para 15-049. See *Director General of Fair Trading v First National Bank* [2002] 1 Lloyd's Rep. 489 at paras 17-20.

<sup>94</sup> *Baird v Eves* [1962] 1 WLR 303, *London Central Limited v. Adrian Smith, Stacy Hill, Darlington* [2004] EWHC 263 QB QBD, at para 28

<sup>95</sup> *Director General of Fair Trading v First National Bank*, *supra* n 93, *per* Bingham L. J., at para 17.

<sup>96</sup> *Ibid* and Beale, H. G., *Chitty on Contracts*, para 15-058

<sup>97</sup> *Director General of Fair Trading v First National Bank*, *supra* n 93, *per* Bingham L. J., at para 17.

<sup>98</sup> Beale, H. G., *Chitty on Contracts*, para 15-049.

a dispute involving a term of a contract for a payment facility, the type of the payment facility involved, whether it is a cheque, a debit or credit card, is a relevant consideration. Similarly, whether the payment is on-line or off-line also has a bearing on the finding of fairness in a disputed term.

The UTCCR also requires the courts to consider other terms of the contract, or the terms of any other contract to which the disputed contract is dependent.<sup>99</sup> For example, Schedule 2 para 1(i) provides that a contract term which irrevocably binds the consumer to terms which he did not know before the conclusion of the contract is *prima facie* unfair. However, by virtue of Reg. 6 (1), the term may pass the UTCCR fairness test if other terms of the contract give the consumer the right to cancel the contract within a cooling-off period without any penalty.<sup>100</sup>

Finally, as a guide to the courts, Schedule 2 of the UTCCR listed 17 types of contract terms that are potentially unfair to the consumer. However, these guidelines are not to be used as a conclusive indication of the fairness of a contract term because as

---

<sup>99</sup> Reg. 6 (1) UTCCR.

<sup>100</sup> Beale, H. G., *Chitty on Contracts*, para 15-056, See for example s. 7.1 of the Banking Code which encourage the issuer to give the consumer the cooling-off period of 14 days after the receipt of the terms and conditions. See also the Natwest credit card terms and conditions at <<https://sol.natwest.com/creditcards/applyonline/ccardlegal.asp>> (Visited 18th August 2005). When the contract for financial services is concluded at a distance such as via the internet or telephone, the issuer is required by Reg. 7(1) of the Financial Services (Distance Marketing) Regulations 2004, SI 2004/2095, to disclose the cooling-off period to the consumer.

mentioned earlier, the fairness of the contract terms depends on various factors surrounding the conclusion of the contract.<sup>101</sup>

In conclusion, both the UCTA and the UTCCR can be used to examine procedural and substantive unfairness of any contract term that affects the allocation of any unauthorised payment between the consumer and the issuer. Although the UCTA and the UTCCR apply a different set of tests, both the reasonableness and the fairness tests are aimed at upholding the principles of fair dealing.

Apart from the UCTA and the UTCCR, the consumer who enters into an agreement for a credit card facility is also protected against an unfair credit agreement by the “unfair relationship” rule in s.140A of the CCA as inserted by s 19 of the Consumer Credit Act 2006 (the “CCA 2006”).

Read together with s. 140B, unfairness under s 140A allows the courts to make an order to alter the terms of the credit agreement or when the terms impose any duty on the consumer to set aside that duty, if it found that the relationship of the parties turned out to be unfair to the consumer because of that term.<sup>102</sup>

It is yet to be seen what is considered as fairness under the new section. However, it is possible that the concept of fairness in s 140A is identical to fairness under the

---

<sup>101</sup> Beale, H. G., *Chitty on Contracts*, para 15-069 and also *Director General of Fair Trading v First National Bank* [2002] 1 Lloyd's Rep. 489.

<sup>102</sup> Section 140A read together with s. 140B (1) (e) (f) and (2) of the CCA 2006.

UTCCR.<sup>103</sup> This is to be understood from the DTI's view of the courts' approach to determine fairness, where it said that courts should take into account various factors that affect the parties' dealing including the issuer's trade practices, the cost of credit, and also the issuer's conduct as a responsible or an irresponsible creditor.<sup>104</sup> Other than that, the consumer's knowledge of the respective terms, his free will to contract, the issuer's effort to explain to the consumer the contract terms, and the effect and the risk of contracting must also be considered in assessing fairness in s. 140A.<sup>105</sup> These factors were among those considered by the court in *Director General of Fair Trading v First National Bank*<sup>106</sup> to test the fairness of the contract under the UTCCR rules.

If the UTCCR concept of fairness applies to the new CCA provision, it will allow the courts to examine the credit agreement for procedural and substantive fairness. Despite the said potential, the scope of the test differs because the fairness test in the CCA is wider than the UTCCR. The latter only examines the circumstances that surround the conclusion of the contract while s. 140A of the CCA allows the courts to consider subsequent events that created the fairness.<sup>107</sup> Probably this rule will give the courts the authority to amend the term of a contract that considered a payment valid when initiated with the use of the consumer's PIN if new developments in technology allow criminals to obtain the PIN and use it to access the consumer's account without the consumer's knowledge.

---

<sup>103</sup> Patient, J., "The Consumer Credit Act 2006" (2006) *J.I.B.L.R.* 21(6), 309, at 312-314.

<sup>104</sup> Department of Trade and industry white paper on "Fair, Clean and Competitive: The Consumer Credit Market in the 21<sup>st</sup> Century", at <<http://www.dti.gov.uk/files/file23663.pdf>> at 52. (Visited 10<sup>th</sup> June 2006).

<sup>105</sup> *Ibid*, at 57.

<sup>106</sup> [2002] 1 Lloyd's Rep. 489 at 496, *per* Bingham L.J.

<sup>107</sup> *Supra* n 104, at 54. See the case study provided in the said White Paper.

## 5 THE MALAYSIAN POSITION

In Malaysia, there is no specific statute that regulates the use of unfair terms. As the law stands now, the use of an exclusion clause is regulated by the incorporation and construction of contract rules.<sup>108</sup>

Although Malaysian law is greatly influenced by English law, yet the application of English law is restricted by virtue of the Civil Law Act 1956 to common law rules, the rules of equity and also the statutes that were administered in England before 1957.<sup>109</sup> Accordingly, in a dispute involving the validity of the terms of a contract, the rules as made by the English courts before 1957 are binding authorities, while decisions thereafter do not have any legal force, except as persuasive authorities.<sup>110</sup> Moreover, the said restriction also means that the UCTA and the UTCCR do not have any influence in Malaysian courts.<sup>111</sup>

---

<sup>108</sup> See above page 4-28. See also Venugopal, A. V., "The Effects of Exclusion Clauses" [2002]2 *CLJ* liii.

<sup>109</sup> Section 3(1)(a) of civil Law Act 1956 provides that the court shall "(a) in West Malaysia or any part thereof, apply the common law of England and the rules of Equity as administered in England on 7 April 1956" "(b) in Sabah, shall apply the common law of England and the rules of Equity, together with statutes of general application, as administered or in force in England on 1st day of December 1951." "(c) in Sarawak, apply the common law of England and the rules of Equity, together with statutes of general application, as administered or in force in England on 12th day of December 1949..." provided they are not inconsistent with local circumstances. See Sinnadurai, V., *The Law of Contract in Malaysia and Singapore: Cases and Commentary*, 2<sup>nd</sup> Edn. (1987) at 209, Butterworths; Alsagoff, S. A. *Principles of the Law of Contract in Malaysia* (1996) Malayan Law Journal, at 107; Phang, A. B. L., *Cheshire Fifoot and Furmston's Law of Contract*, 2nd (1998) Malayan Law Journal, at 41-42.

<sup>110</sup> Ibid.

<sup>111</sup> See *Wee Lian Construction Sdn Bhd V Ingersoll-Jati Malaysia Sdn Bhd* [2005] 1 MLJ 162, at 176 - 178, (the "Wee Lian Construction") and *Standard Chartered Bank v Boomland Development Sdn Bhd & Others* [1997] 4 AMR 3442.

Moreover, the codification of the common law of contract into the Contract Act 1950 means that the courts must apply the rules as incorporated in the statute to analyse the validity of a contract or its terms.<sup>112</sup> This position was confirmed in *Yewpam Sdn Bhd v Mohd Salleh Bin Sheikh Ahmad & Anor*<sup>113</sup> where the court emphasised that since s.16 of the Contract Act 1950 already regulates the formation of a contract affected by undue advantage through the undue influence rule, the court is not free to apply the English doctrine of inequality of a bargaining position to assess the validity of a contract.

It should be noted that although before the *Yewpam* case the Court of Appeal in *Saad bin Marwi v Chan Hwan Hua & Anor*,<sup>114</sup> had applied the doctrine of inequality of a bargaining position to reach its decision, it is yet to be seen the extent to which the decision will be followed. The *Yewpam* case and that of *American International Assurance Co Ltd v Koh Yen Bee (F)*,<sup>115</sup> which came after it, however, demonstrated the courts' strong rejection of applying English rules of assessing the enforceability of a contract or its terms in Malaysia.

Based on the above discussion it is clear that in Malaysia, the incorporation and construction of contract rules, apart from the rules that are concerned with free consent to contract, continue to provide the avenue for contracting parties, consumers or businesses to challenge the enforceability of their contract or its terms.

---

<sup>112</sup> Section 14 -19 of the Contract Act 1950.

<sup>113</sup> [2001] 1 LNS 43, Para 17.

<sup>114</sup> [2001] 3 CLJ 98, at 115-116.

<sup>115</sup> [2002] 4 MLJ 301, at 319.

## 6 ANALYSIS OF THE ELECTRONIC PAYMENT CONTRACT TERMS

All of the electronic payment regulations discussed in the previous chapters prescribe specific conditions, methods and procedures for allocating unauthorised payments between the consumer and the issuer. Accordingly, the contract between the consumer and the issuer must contain terms that incorporate these rules. Despite the importance of the rules, some of the regulations discussed do not render ineffective the contract terms that contradict their rules. Unless other rules can be applied to invalidate the contradictory terms, the consumer may be unfairly burdened with the losses caused by unauthorised payment. In some jurisdictions, as shown in the previous discussion, the problem can be remedied by applying the rules which regulate the use of unfair terms.

Among the contract terms which may contradict the regulatory loss allocation rules are terms found in an exclusion clause, a limitation of liability clause, and an indemnity clause. Moreover, clauses that regulate the termination of a card user's authority and the cancellation of a payment card, and clauses that describe the condition for liability may also affect the fair allocation of unauthorised payments. Another clause which may have an impact on the allocation of unauthorised payment losses is a conclusive evidence clause.

In the following discussion, the aforementioned clauses, chosen from various credit and debit card terms and conditions used by Malaysian issuers will be analysed to identify their impact on the consumer. The terms will be examined from the fairness perspective

using the unfair contract terms' rules as the benchmark. It should be observed that although the discussion is concerned only with some clauses, it does not mean that other clauses are free from unfairness. The clauses were chosen for three reasons. First, these clauses contain terms that are closely associated with loss allocation. Second, since the Malaysian credit card and EFT loss allocation rules suffer from a lack of clarity,<sup>116</sup> and unclear rules are hard to follow, the terms chosen reflect the insufficiency of the rules and the potential disadvantages faced by Malaysian consumers. Finally, the CC and EFT Guidelines also do not invalidate any contradictory contract terms. A lack of penalty provision allows the issuer to insert its own loss allocation rules in its contract terms. These contradictory terms may jeopardise the protection of the consumer against unauthorised payment.

## **A Contract Terms that Affect the Protection of the Consumer against Unauthorised Payment**

### *(a) Exclusion or limitation of a liability clause*

In a contract between a consumer and the issuer of electronic payment facilities, it is common for the issuer to insert into its contract terms a clause that limits its losses while allocating the rest to the consumer. However, all loss allocation rules discussed in Chapter three restricted the issuer's right to do so. These rules required the issuer to

---

<sup>116</sup> See chapter 3 and 4 discussion



incorporate into its contract terms clauses which limit the consumer's liability to a specific capped amount of losses.<sup>117</sup>

A brief review of several credit card and EFT contract terms used by issuers in the United States and the United Kingdom revealed the issuers' strict compliance with the rules that capped the consumer's losses.<sup>118</sup> The said effect is achieved because the TILA, the EFTA and the CCA rules make contradictory contract terms unenforceable.<sup>119</sup> The same issuers' attitude can also be identified in the contract for EFT payment facilities in the United Kingdom although the Banking Code does not prevent the use of other loss allocation rules. Perhaps this behaviour is encouraged by the issuers' fear of being accused of breaching their promise to act fairly in their dealings with the consumer, which includes using fair contract terms and conditions.<sup>120</sup> Moreover, this attitude may also have been influenced by the Ombudsman's recognition of the superiority of the Code over the issuers' contract terms.<sup>121</sup>

In the case of EFT payments in distance transaction, contract terms which purport to allocate to the consumers losses in excess of the capped amount should not be

---

<sup>117</sup> Section 133 of the TILA and s. 909 of the EFTA provided that any agreement that purport to allocate losses to the consumer beyond the amount specified therein is void. Section 173 of the CCA also renders an agreement which allocates to the consumer a bigger amount of losses than allowed therein as void.

<sup>118</sup> See for example clause 7.3 of the Egg card New Credit Agreement, <[http://new.egg.com/visitor/0,,3\\_11087--View\\_1068,00.html](http://new.egg.com/visitor/0,,3_11087--View_1068,00.html)>, clause 4 of the Royal Bank of Scotland credit card terms and conditions at <https://personal.rbs.co.uk/ImportantInfo/creditcards.asp>, Clause 15 of First Citizen Bank at <<http://www.fcbl.com/ccdisclosure.asp>> and clause 19 of CorTrust Bank at <<http://www.cortrustbank.com/CreditCards/DownloadApplications/VISAGold/Index.cfm>> (Visited 25<sup>th</sup> June 2006).

<sup>119</sup> See s. 133 (d) of the TILA s. 909 (1)(e) of the EFTA, s. 173 of the CCA.

<sup>120</sup> Section 2 and 6.2 of the Banking Code.

<sup>121</sup> Ombudsman News at <<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/9/sept-disputed-cash-machine-withdrawals.htm>> (Visited 26<sup>th</sup> June 2006).

enforceable because of the reasons mentioned above. Moreover, the terms also contradict Reg.21 of the DSRs which allocate all unauthorised payment losses to the issuer.

Malaysian consumers' situation is entirely different from consumers in the United States and United Kingdom. For instance, in the case of a credit card payment facility, the CC Guidelines capped the amount of consumers' losses to a maximum of RM250 of the total amount of loss incurred before the issuers received notice of an unauthorised payment.<sup>122</sup> However, some issuers allocate the entire amount of an unauthorised payment to the consumer. For example, clause 6 of the Affin Bank credit card agreement provides:<sup>123</sup>

"The Cardmember shall be liable for all transactions incurred from unauthorised usage of the card until a report of loss or theft has been received by the Bank."

An identical term is found in many other terms and conditions including clause 9.2 of the AmBank Al-Taslim Master/Visa Terms and Conditions.<sup>124</sup> The most extreme clause is the Maybank credit card terms and conditions which states:<sup>125</sup>

---

<sup>122</sup> Paragraph 13.2 of the CC Guidelines.

<sup>123</sup> Clause 6. of the Affin Bank's Classic/Gold/Platinum/MasterCard/VISA credit card) terms and conditions, at <<http://www.affinbank.com.my/ccards/terms.htm>> (Visited 20<sup>th</sup> June 2006).

<sup>124</sup> On file with the researcher. See also Citibank Clause "Disclosure of PIN, or Loss, Theft or Unauthorised Use of Card" of the Citibank Visa and Mastercard terms and conditions" at <[https://www.citibank.com.my/APPS/portal/genericLoadPage.do?tabNo=3&htmlPageName=/info/det/creditcard\\_tnc.htm](https://www.citibank.com.my/APPS/portal/genericLoadPage.do?tabNo=3&htmlPageName=/info/det/creditcard_tnc.htm)> (Visited 20<sup>th</sup> June 2006).

<sup>125</sup> Clause 3.4 (c) of the Maybank Gold Card Agreement at <[http://www.maybank2u.com.my/consumer/online\\_cards/agreement\\_gold.pdf](http://www.maybank2u.com.my/consumer/online_cards/agreement_gold.pdf)> (Visited 20<sup>th</sup> June 2006).

“[T]he Cardholder shall be liable for all charges and advances whatsoever arising from all transactions, whether authorised or unauthorised, effected with the Credit Card.”

All these terms clearly contradict Para 13.2 and 13.3 of the CC Guidelines which allow the issuer to allocate more than RM250 of losses to the consumer, only when the losses were caused by the consumer’s fraud or negligence.

These terms continue to be used although s. 57 of the Payment Systems Act 2003 makes non-compliance with the CC Guidelines an offence.<sup>126</sup> Since the terms discussed are current, it shows that the CC Guidelines and the Payment Systems Act are ineffective in protecting the consumer against contractual terms that contradict the CC Guidelines and are unfair for the consumer.<sup>127</sup>

Apart from acting in defiance of the CC Guidelines and the Payment Systems Act, the issuer’s usage of the contradictory terms is also against public policy.<sup>128</sup> Furthermore, the terms discussed in the above paragraphs reflect the issuer’s total disregard for the risks of fraudulent payment, which may originate from various sources and not necessarily by the consumer’s fault. For example, credit card payment usually

---

<sup>126</sup> Section 57 read together with s. 70 and s.77 (4) showed the duty of the issuer to comply with the Guidelines.

<sup>127</sup> See the Citibank terms and conditions at <[https://www.citibank.com.my/APPS/portall/genericLoadPage.do?TabNo=3&htmlPageName=/info/det/creditcard\\_tnc.htm](https://www.citibank.com.my/APPS/portall/genericLoadPage.do?TabNo=3&htmlPageName=/info/det/creditcard_tnc.htm)>; the Affin Bank terms and conditions at <<http://www.affinbank.com.my/ccards/terms.htm>>; (Visited 20<sup>th</sup> June 2006), and the Ambank terms and conditions on file with the researcher.

<sup>128</sup> Abdul Hamid J. in *Banque Nasionale De Paris v Wuan Swee May & Anor* [2000] 3 MLJ 587, at 597, emphasised that the issue of public policy is a country-based analysis. Therefore, in Malaysia, the court has to examine the Malaysian law, the Malaysian government policy, Malaysian moral values and all other relevant factors prevailing in Malaysia, including the economic and educational development of the citizen, political and social problems, culture and religion and also the attitude of the general public and the government towards religion.

necessitates the consumer bringing along the card to the point of transaction. In this circumstance, it is not inconceivable that the consumer could be exposed to the risk of loss or theft of the card. Therefore, any contract term that allocates unauthorised payment losses to the consumer, without taking into account different types of risk, is unfair. It is so because it allocates to the consumer a risk which is outside his control. This type of contract term is injurious to the consumer, considering that a credit card contract is a non-negotiable standard form contract.

Notwithstanding the grave impact of the above terms on the protection of the consumer against unauthorised payment, the consumer's only alternative in avoiding the said contract terms is to challenge their validity by applying the incorporation and the construction of contract rules.

However, the incorporation of contract rule which examines the contractual formation process can do little to protect the consumer, unless the terms are printed in very fine print or they were not disclosed to him. Since contract terms are either disclosed in the credit card application form, or in other cases, they are given to the consumer, together with the credit card approval notification, of course, with a right to cancellation, the terms most of the time satisfy the common law rule of contractual incorporation.<sup>129</sup>

The final alternative is for the courts to determine the parameter of the consumer's liability for an unauthorised payment within the relevant contract terms. In this regard,

---

<sup>129</sup> *Sanggaralingam Arumugam v. Wong Kook Wah & Anor* [1987] 2 CLJ 255, at 256.

the common law rules require the courts to examine the circumstances surrounding the contract at the time of its conclusion to construe the meaning to be given to the contract terms.<sup>130</sup> The circumstances to be considered include the nature of the contract, the language of the disputed terms, the practice of the relevant industry, and other terms of the said contract.<sup>131</sup> These factors may reveal the parties' true intention at the time of contracting.

By applying the construction of contract rule, the scope of the terms quoted above may be used to allocate losses bigger than the capped liability to the consumer, only when the losses were by his fault. However, these terms should not be used to make the consumer liable for bigger losses when the losses were the fault of the issuer or third party. In particular, the terms quoted in this discussion must not be used to protect the issuer against losses caused by its negligence since the language used did not clearly say so.<sup>132</sup>

Nonetheless, the suggested interpretation may be of little significance considering that some terms are expressed using very far-reaching words. For example, clause 3.4 (c) of the Maybank's credit agreement<sup>133</sup> contains words which catch all losses caused by

---

<sup>130</sup> *Hwa Chea Lin & Anor v Malim Jaya (Melaka) Sdn Bhd* [1996] 4 MLJ 544, *Associated Concrete Products (M) Sdn. Bhd. v. Tackoh Sdn. Bhd* [1992] 2 CLJ (Rep) 133, and *Talam Leasing Sdn. Bhd. v. Batu Wong Koon Sdn. Bhd. & Ors.* [1988] 2 CLJ (Rep) 455, at 460, *per* Gunn Chit Tuan J.

<sup>131</sup> *Lee Yee Yew v. United Oriental Assurance Sdn. Bhd. & Another* [1998] 4 CLJ 763; *Marine' v. Owners of and other persons interested in the ship or vessel 'Taveechai Marine'* [1995] 1 CLJ 720

<sup>132</sup> *Kuok Ling Timber Industries Sdn Bhd v The Owners of and other Persons Interested in the Vessel "My Thonfullin"* [2000] 2 MLJ 615, at 633-634.

<sup>133</sup> Maybank Gold Card agreement at <[http://www.maybank2u.com.my/consumer/online\\_cards/agreement\\_gold.pdf](http://www.maybank2u.com.my/consumer/online_cards/agreement_gold.pdf)>. (Visited 25<sup>th</sup> June 2006).

unauthorised credit card payment regardless of the manner of its occurrence. It provides:

“the Cardholder shall be liable for all charges and advances *whatsoever* arising from all transactions, whether authorised or unauthorised, effected with the Credit Card.” [Emphasised added]

The issuer may rely on this clause to allocate all losses to the consumer even when the losses were caused by its own negligent conduct.<sup>134</sup>

Apart from the language used, the courts may also refer to other clauses in the contract to construe the scope of the consumer’s liability. For instance, the Maybank notification clause which provides:

“If the Credit Card is lost or stolen, the Cardholder shall notify ... immediately upon the discovery of such loss or theft...Until and unless such written confirmation has been received by Maybank, the Cardholder shall remain liable for all charges incurred prior thereto by the use of the Credit Card whether authorised by the Cardholder or not”,

may be read together with clause 3.4 to limit the consumer’s liability to losses incurred before the issuer received notification of loss or theft of the consumer’s credit card.<sup>135</sup>

However, that approach does not necessarily help in every case. Some contract terms that are concerned with notice of potential losses may lend support to the construction of

---

<sup>134</sup> *PremierHotel Sdn Bhd v Tang Ling Seng* [1995] 4 MLJ 229, at 232.

<sup>135</sup> Clause 8.3 of the Maybank’s agreement at <[http://www.maybank2u.com.my/consumer/online\\_card\\_s/agreement\\_gold.pdf](http://www.maybank2u.com.my/consumer/online_card_s/agreement_gold.pdf)> (Visited 25<sup>th</sup> June 2006).

the loss allocation term in favour of the consumer. Others may not be so useful. For example, one of the issuers provides in its contract:<sup>136</sup>

“...we may resolve that your liability be limited to RM250.00 ...in respect of only transactions effected through the use of your Card for the period of one (1) hour prior to you reporting to us the loss or theft or unauthorised use of your card on proof that you had in good faith exercised reasonable care and diligence to prevent such loss, theft or unauthorised use of your Card and had promptly reported the loss or theft or unauthorised use of your Card to us.”

This contract term appears to be beneficial to the consumer as it limits his liability to RM250. However, it allows the issuer to allocate unauthorised payment losses based on negligence, contrary to the CC Guidelines, which do not contain negligence-based loss allocation rules.<sup>137</sup> Moreover, the term also shows the issuer’s intention to allocate to the consumer all losses except those incurred an hour prior to the notification.

The issuer’s non-compliance with the Guidelines’ loss allocation rules is also identified in the contract for debit card facility. The EFT Guidelines allow the issuer to allocate to the consumer only those losses that were incurred before the notice of loss or theft of the card was given to the issuer. However, some issuers failed to include this term in their contract. Clause 7 of one of the issuers provides:<sup>138</sup>

---

<sup>136</sup> Citibank credit card agreement, “Disclosure of PIN, or Loss, Theft or Unauthorised Use of Card Disclosure of PIN, or loss, theft or unauthorised use of card”, at <[https://www.citibank.com.my/APPS/portal/genericLoadPage.do?tabNo=3&htmlPageName=/info/det/creditcard\\_inc.htm](https://www.citibank.com.my/APPS/portal/genericLoadPage.do?tabNo=3&htmlPageName=/info/det/creditcard_inc.htm)> (Visited 25<sup>th</sup> June 2006).

<sup>137</sup> Paragraph 13 of the CC Guidelines which contains loss allocation rules, does have a negligence-based rule.

<sup>138</sup> See for example Clause 7 of the OCBC Bank Electronic Services. Electronic Service is defined to include the use of the card at the ATM, terminal or counter or terminal maintained by approved person. On file with the researcher.



“The customer shall be responsible and liable for all withdrawal of cash or transfer of funds or balance enquiries or transaction made or performed or processed or effected by or with the use or purported use of the Electronic Services whether with or without the customer’s knowledge or authority”

In this clause, the issuer allocates all unauthorised payment to the consumer. The use of this clause which exposed the consumer to an unlimited amount of losses is facilitated by the flaw in the EFT Guidelines which did not cap the consumer’s liability at a certain amount as it did in the CC Guidelines. The issuer, however, ignored the rule in Para 15.3 and Para 16 of the Guidelines which tied the consumer’s liability to the timing of notification. If the notification rule is incorporated in the contract terms, Clause 7 can be construed to limit the consumer’s liability to the losses incurred before he informed the issuer of the events stipulated by the notification clause. However, a search through the contract terms revealed nothing to that effect as they lack a notification clause. Consequently, the consumer cannot limit his losses by informing the issuer of the events that may facilitate unauthorised payment.

A failure to disclose the notification method to the consumer is an offence under s. 57 of the Payment Systems Act, and is punishable by a fine. Nevertheless, this type of clause continues to be used by the issuer; indicating weaknesses in the implementation of the Payment Systems Act.



The above loss allocation clause is also unfair on the consumer because of its confusing description of one of the methods of initiating unauthorised payment namely; the “purported use of the electronic service”.

“Electronic service” in the issuer’s contract terms, was defined to include the use of a debit card to pay for the sale of goods or supply of services.<sup>139</sup> Reading this definition together with the word “purport”, which literally means to imply or convey or to have the appearance of being; which refers to a thing or act which is not real”<sup>140</sup> the above clause allows the issuer to allocate to the consumer losses caused by an unauthorised payment initiated with the use of a card which appeared to be the consumer’s. If this is the proper construction of the clause, the consumer is liable for the transaction initiated with the use of a clone card. If the card refers to the card issued to the consumer and the word “purport” is read with the word “use”, the clause can also be relied on by the issuer to allocate any unauthorised payment initiated by whatever way that appeared to be initiated, by using the consumer’s card.

From the above, it can be concluded that using the common law rules of incorporation and construction of contract to determine the enforceability of a contract or its terms has a negative impact on the protection of the consumer against unfair terms. This is so because the courts’ authority to question the fairness of a contract or its terms is limited

---

<sup>139</sup> Clause 28 of the OCBC terms and conditions.

<sup>140</sup> *Public Prosecutor v Hoo Chee Keong* [1997] 4 MLJ 451, at 461- 462.

only to situations where the contract formation process has failed to meet the legal requirements.

A lack of unfair terms regulation, coupled with weaknesses in the implementation of the electronic payment Guidelines and the Payment Systems Act seriously affect the protection of the consumer against unauthorised payment. Therefore, unless the contract terms which contain an exclusion or a limitation of liability clause also contain a notification clause, which can help in the construction of the exclusion or the limitation of a liability clause, the consumer may face the risk of unlimited losses without being given the opportunity to prevent or to avoid the losses.

Another weak point of the CC and EFT Guidelines is that they do not regulate the - allocation of an unauthorised payment in distance transactions, where neither the card nor the associated PIN was used.<sup>141</sup> The contract terms reviewed in this study showed that the issuers adopted different approaches in allocating unauthorised payments made in distance transactions. The common scheme is to allocate all losses to the consumer. For instance, one of the sample contract terms provides:<sup>142</sup>

“If you use your Card to purchase goods and/or services through the online internet sites or portals, you shall be solely responsible for the security of such use at all time. You agree that the entry of your card information on the internet shall be sufficient proof of the authenticity of such instructions. We shall not be under any obligation to verify the identity or the authority of the person entering your Card information and we shall not

---

<sup>141</sup> Chapter two at 64.

<sup>142</sup> Internet Transaction Clause of the Citibank Malaysia Credit Card Terms and Conditions.

be liable for acting on such use regardless of the circumstances prevailing at the time of the transaction....”

This exclusion clause contains many parts which all resulted in the allocation of unlimited losses caused by unauthorised internet payments initiated using the card details. In particular;

(a) the issuer totally disregarded the risk of an internet security breach which may occur not only at the consumer’s end but along the communication line and at the issuer’s own end;

(b) the issuer also ignored the fact that card details can be easily obtained by others without that being the consumer’s fault;

(c) the issuer refused to take responsibility to develop a suitable and secure authentication system although it profited from online commercial activities; from the fees paid by the merchants with whom it had entered into merchant agreements. The issuer should be responsible in some circumstances because it is in a better position, compared to the consumer, to take steps to reduce or prevent losses because it has the financial and technical ability to innovate or adopt secure technology;<sup>143</sup>

(d) the issuer protects itself against losses which may have occurred as a result of the system security breach caused in return by its failure to maintain the security; and finally;

---

<sup>143</sup> Cooter, R. D. and Rubin, E. L., “A Theory Of Loss Allocation For Consumer Payments”, at 73-77.

(e) the issuer also protected itself against liability for unauthorised payment even though the payment was facilitated by its failure to use authentication technology to verify the authority of the person who used the consumer's credit card details.

Despite the appalling effects of the above contract terms, its incorporation in the issuer's contract does not contravene s. 57 of the Payment Systems Act because the CC Guidelines did not regulate the allocation of unauthorised payment in distance transactions.

Even if the clause were to be examined from the incorporation of contract rules it will pass through because it is common practice in the credit card industry for the terms and conditions to be given to the consumer at the time his application is approved with the right to cancellation.<sup>144</sup> Similarly, if the clause is to be construed to find its true meaning, it is probable that it will also pass the courts scrutiny because the language used clearly excluded the issuer from being liable for the losses caused by any unauthorised internet payment initiated using the credit card details.

Eventually, the consumer is faced with the choice of being totally responsible for an unauthorised payment made in a distance transaction or having to avoid using a distance payment facility. However, to force the consumer to make this choice, especially if the subject matter of the contract is essential, is unfair.

---

<sup>144</sup> Above page 260, and accompanying note, n 129.

(b) *Indemnity clause*

An indemnity clause is a clause in which one party promises to make good any loss which the other party suffers as a consequence of his act or default.<sup>145</sup> This type of clause is usually used by the issuer to claim the cost and expenses it has incurred in enforcing the agreement against the consumer. However, in some circumstances, the issuer uses the clause to claim more than that. For instance, one issuer provides:<sup>146</sup>

“The Cardmember acknowledges and agrees that he shall be fully responsible and liable for all transactions effected by the use of the PIN whether with or without the knowledge or authority of the Cardmember and *shall indemnify and keep RHB Bank fully indemnified against all consequential losses, expenses or claims suffered by or brought against RHB Bank.*” [Emphasis added]

This clause requires the consumer to make up the cost incurred by the issuer not only in enforcing the agreement against the consumer when the consumer was at fault but also in cases where the payment was unauthorised. Moreover, the issuer may rely on this clause to claim indemnification for the cost it has incurred in its dispute with merchants over its right to chargeback the payment when the consumer disputed the payment for lack of a proper mandate.

---

<sup>145</sup> Section 77 of the Malaysian Contract Act 1950. See also *The Pacific Bank Bhd v Vimla Textiles & Ors* [2004] 6 CLJ 406.

<sup>146</sup> Clause 2.4 of the RHB banks terms and conditions. On file with the researcher.

Another issuer provides:<sup>147</sup>

“The consumer undertakes with the Bank and agrees to indemnify the bank from and against and in respect of all liabilities losses charges and expenses (including legal fees and costs on a solicitor and client basis) claims demands actions and proceedings which the Bank may incur or sustain directly or indirectly from or by reason of or in relation to the use or purported used of the Electronic Services whether with or without the Customer’s knowledge or authority or arising out of or in consequence of the Customer’s negligence or any act or omission on the part of the Customer or any breach of these terms and conditions or by reason of or in consequence or any access or attempted access or purported access to the Electronic Services and the Customer shall pay such sums on demands.”

This indemnity clause also has a far-reaching effect. It especially allows the issuer to claim its cost of trying to demand repayment from the consumer for unauthorised payment regardless of the fact that the payment may have not been caused by the consumer’s fault or by a breach of the conditions of liability. Similarly, the clause also requires the consumer to indemnify the issuer against the losses which the latter may suffer when an unauthorised individual attempts to access the consumer’s electronic services.

The above two indemnity clauses, one in a credit card agreement and another in an agreement governing the use of debit card, indirectly allocate to the consumer the issuer’s cost relating to unauthorised payment.

Other than the above, the indemnity clauses quoted also contradict the CC and EFT Guidelines which allocate unauthorised payment losses to the consumer only in certain

---

<sup>147</sup> Clause 19 of the OCBC electronic services terms and conditions. On file with the researcher.

circumstances. For example, the CC Guidelines allocate unauthorised payment to the consumer if he failed to inform the issuer of the loss or theft of the credit card within a reasonable time or when the consumer had acted fraudulently.<sup>148</sup> On the other hand, the EFT Guidelines allow the issuer to allocate the losses to the consumer in one of these circumstances; when the consumer fails to exercise reasonable care in keeping the access code confidential; or he fails to comply with the strict duty of maintaining the confidentiality of the PIN or the electronic access device; or he fails to inform the issuer of the events that may facilitate unauthorised payment.<sup>149</sup>

Despite having specific rules governing the allocation of unauthorised payment, both Guidelines do not render unenforceable any term that contradicts their provisions. Hence, the issuers may choose to enforce their unfair contract terms on the consumers and face a penalty under s. 57 of the Payment Systems Act.

*(c) Conditions of Liability*

Other than the exclusion clause, the limitation of liability clause and the indemnity clause credit card agreement and the agreement for debit card facility also contain terms which describe the circumstances in which the consumer is liable for any unauthorised payment.

---

<sup>148</sup> See the discussion in Paras 13. and 13.3 of the CC Guidelines.

<sup>149</sup> Paragraphs 15 and 16 of the EFT Guidelines.

For instance, the contract may require the consumer to protect the security of the payment devices or the access code. A failure to perform this duty will make the consumer liable for any unauthorised payment initiated with the use of the access device and/or the code. This type of term is found in all terms and conditions reviewed in this study; the EFT payment system and the credit card system alike, although only the EFT Guidelines have fault-based loss allocation rules.<sup>150</sup>

Because the terms which described the conditions for liability affect the allocation of unauthorised payment losses, it is not too extreme to suggest that unfair loss allocation conditions affect the protection of the consumer against unauthorised payment. The following are some conditions used by the issuers to determine consumers' liability for unauthorised credit or debit card payments.

*(i) Protection of PIN confidentiality*

Initially, only the EFT Guidelines allocate losses based on the consumer's failure to protect the confidentiality of his PIN.<sup>151</sup> The CC Guidelines, on the other hand, allocate unauthorised payment losses by looking at the unauthorised nature of credit card usage and the fraudulent act of the consumer.<sup>152</sup>

---

<sup>150</sup> See Chapter three at 135-138 and Para 15(1) (b) of the EFT Guidelines.

<sup>151</sup> See Chapter three at 135-138.

<sup>152</sup> Ibid at 118-120.



Nevertheless, the practices of the issuers in both the EFT and credit card payment systems are identical since they equally require the consumer to protect the PIN to avoid the losses. For instance, one debit card issuer provides in its contract terms: <sup>153</sup>

“... the cardholder must never reveal his/her PIN to anyone, including the Bank’s personnel, and it should not be kept together with the card but committed to memory.”

Failing to observe this obligation, the consumer will be liable for all losses caused by unauthorised use of his card, which is lost or stolen, together with the PIN.<sup>154</sup> This clause may catch the consumer who wrote down the PIN and kept it together with his card that is lost or stolen. It indirectly and unfairly penalises the consumer for failing to memorise the PIN without considering that some consumers may not have the ability to do so.

Another debit card issuer states:<sup>155</sup>

“The Cardholder shall at no time and under no circumstances *reveal or cause to reveal* the PIN to any other person including the Bank’s personnel.” [Emphasised added]

The word “reveal” in ordinary plain English means to “disclose, or cause or allow to be seen”.<sup>156</sup> Hence, “reveal” may cover active and passive behaviour that enables the PIN to be seen by others, including, for instance, failing to shield the PIN from others’ view

---

<sup>153</sup> Clause 4 read together with Clause 7 of the BCB PMPC-ATM card terms and conditions. On file with the researcher.

<sup>154</sup> Ibid, clause 5(b), supra n 138, Clause 7.

<sup>155</sup> Clause 3(b) of the BIMB Bank Smart BIMB Account/Card Agreement terms and conditions. On file with the researcher.

<sup>156</sup> Pearsall, *The Concise Oxford Dictionary*, at 1224.

while using it at the ATM or the EFTPOS terminal.<sup>157</sup> Unless the issuer can make sure that the terminal at which the card and the PIN are used is perfectly secure against any type of risk including the risk of illegal recording, the clause is unfair on the consumer as it was drafted without considering the inherent risk of transacting at terminals located in public places.<sup>158</sup> The above clause may affect the consumer who is a victim of cloning activities; where the PIN was stolen to be used with the cloned card.<sup>159</sup>

Sometimes, credit card issuers allocate unauthorised payment to the consumer by imposing on the consumer a duty to maintain the secrecy of the PIN. For instance, one credit agreement provides:

“...The PIN is strictly confidential and should not be disclosed to any person under any circumstances by whatever means”.<sup>160</sup>

This term is very wide and extensive as it subjects the consumer to an uncertain scope of duty and responsibility. Consequently, the consumer will have difficulty in visualising the action that he is supposed to take or to abstain from in performing this duty.

---

<sup>157</sup> The dispute term is to be given its plain ordinary meaning. See for example in *MBF Insurans Sdn Bhd v Penang Garden Sdn Bhd* [2004] 4 MLJ 345, at 356 where the Court of Appeal defined the word “collapse”, used in a building insurance, to refers to its ordinary meaning relying on the definition given in a dictionary saying that “when the words of [agreement] are crystal clear, those words must be given effect to.” See also *Devi Nadchatiram v Saraswathy Devi Nadchatiram* [2000] 4 CLJ 870, *Rs Muthiah v Pembinaan Fiba Sdn Bhd* [2004] 4 MLJ 78 and *Hoya Holdings Sdn Bhd v Chia Thin Hing @ Cheah Thin Heng & Anor* [1994] 4 CLJ.

<sup>158</sup> Cooter, R. D. and Rubin, E. L., “A Theory Of Loss Allocation For Consumer Payments”.

<sup>159</sup> See *Hoo Chee Keong v Public Prosecutor* (No 2) [2000] 5 MLJ 448 and *Wong Kim Leng v Public Prosecutor* [1997] 2 MLJ 97, two out of the many cases which proved that forgery of payment cards especially the credit card is a major problem faced by the electronic payment industry in Malaysia.

<sup>160</sup> Clause 2.4 and 9.1 of the RHB and Clause 2.5 of the AmBank.

The issuer should be encouraged by the Guidelines to use terms that have an element of educating the consumer in the way to protect the PIN but not to use terms that outrightly punish him for using the wrong terminal at the wrong time. For instance, the issuer can use a clause that requires the consumer to write the PIN in a way that cannot be understood by others. The clause should be like:<sup>161</sup>

“The Cardmember shall be fully responsible and liable for all transactions effected by the use of the PIN. *The Cardmember is to take all reasonable precautions to prevent fraudulent use of their PIN. These include:*  
*NEVER disclose the PIN on the card or any other item normally kept with the card*  
*NEVER write the PIN in a way that can be easily understood by any third party...*”  
[Emphasis added]

(ii) Notification clause

Other than the above condition, some contract terms also imposes on the consumer a strict duty to inform the issuer of certain events before the consumer can avoid liability for the unauthorised payment. For example, clause 9.1 of the RHB Bank credit terms and conditions, read together with clause 9.2 provides:<sup>162</sup>

“In the event of any loss or theft or unauthorised use of the Card or the disclosure of the PIN to any unauthorised person the Cardmember shall *immediately* notify the RHB Bank Card Centre *as soon as possible*. A police report should be made for the lost or stolen card or unauthorised use of the card and a copy extended to RHB Bank Card Centre”

---

<sup>161</sup> See Clause 2.6 of the AmBank Berhad MasterCard/Visa agreement. On file with the researcher.

<sup>162</sup> This clause can also be found in Clause 9.1 and Clause 9.2 of AmBank credit agreement, although not identical. The AmBank even requires the consumer to confirm verbal notification in writing. See similar terms in Clause 6.2 and Clause 6.3 of the AFFIN.

This contract term requires the consumer to tender a police report, together with the notice of the events that may facilitate an unauthorised payment to the issuer. Although the CC and EFT Guidelines<sup>163</sup> provide that notification of loss or theft of the card is effective to limit the consumer's liability for an unauthorised transaction, the above term imposes an extra duty to prevent unauthorised payment on the consumer.<sup>164</sup>

The term is substantively unfair because it allows the issuer to allocate the losses that occurred after it had received a notice of loss, theft or unauthorised use of the consumer's card to the consumer when the notice was not accompanied by a police report. This term does not reflect the reality that information given in the notice is usually sufficient to enable the issuer to act to reduce or prevent the risk of unauthorised payment.

Moreover, the above notification clause is also ambiguous in its lack of a specific notification period. This is believed to be the effect of the EFT and CC Guidelines which do not have explicit rules on that matter. Both Guidelines prescribed the modes of measuring the promptness of the notice by requiring the consumer to give notice "without delay" or "as soon as reasonably practicable".<sup>165</sup> Because of this broad standard of promptness, the issuer has discretion to describe the notification period by using phrases that are hardly understood by the consumer.

---

<sup>163</sup> See paragraph 16 of the EFT Guidelines and paragraph 13.2 of the CC Guidelines.

<sup>164</sup> Paragraph 15 (3) and 16 of the EFT Guidelines and para 13. 2 and 13.4 of the CC Guidelines.

<sup>165</sup> Paragrapah 13.2 of the CC Guidelines and para 16 of the EFT Guidelines.

It appears that some phrases used by the issuer in the reviewed terms and conditions do not give a clear idea as to the period considered to be an appropriate notification period. It is unlikely that a phrase such as “shall immediately notify the [issuer] as soon as possible,”<sup>166</sup> would be fully understood by the consumer, not until a dispute arose and the matter is referred to the court or to the Mediation Bureau for settlement. In this situation, it becomes impossible for the consumer to understand the importance of his notice in preventing or reducing the risk of losses.

Furthermore, the use of two conflicting standards of notification period, namely, “immediately” and “as soon as possible”; where “immediately” means “at once, very close or adjacent in time ...”<sup>167</sup> and without “further ado”<sup>168</sup> and “as soon as possible” means “within a reasonable time, the shortest practicable”, “as soon as may be” but not “as late as possible”,<sup>169</sup> make it difficult for the consumer to determine whether the notice given was within the period that allows him to claim the limited liability protection.

Apart from the above issue, it is also uncertain whether by using “immediately” and “as soon as possible” together, the issuer would consider extended travel or hospitalisation

---

<sup>166</sup> See above page 276 and n 162.

<sup>167</sup> Pearsall, J., *The Oxford Concise Dictionary*, at 709.

<sup>168</sup> *Tai Kim Yew & Ors v Sentul Raya Sdn Bhd* [2004] 4 MLJ 227, at 233.

<sup>169</sup> *Chong Co Sdn Bhd v Majlis Perbandaran Pulau Pinang* [2000] 5 MLJ 130, at 135, the judge said, “Obviously, what amounts to ‘as soon as possible’ varies from case to case.”

as a valid excuse for delaying the notification since neither the EFT nor CC Guidelines contain any rule to that effect.<sup>170</sup>

The worst of all the reviewed credit card and debit card terms and conditions are those which do not have any notification clause at all. These terms and conditions do not require the consumer to inform the issuer of any possible unauthorised use of the card and/or the PIN.<sup>171</sup> The issuer for this matter has failed to provide the consumer with the fair opportunity to act to minimise the risk of an unauthorised payment. Moreover, the issuer also fails to comply with Para 6 (4) (a) and (b) and Para 16 of the EFT Guidelines which allocate only a limited amount of losses to the consumer if he had informed the issuer of the events which may facilitate an unauthorised payment. Since the contract terms do not have any notification provision, the issuer may, at its discretion, choose to allocate to the consumer any amount of loss, regardless of receipt of information of any potential unauthorised payment.

(iii) *Return of the card*

Another term frequently incorporated in the contract for electronic payment facilities is a term which imposes on the consumer the duty to return to the issuer the card issued to an additional cardholder. This duty must be performed before the consumer can effectively

---

<sup>170</sup> In the United States of America these two factors are extenuating factors which the consumer can use in defending his delay in giving notice of potential unauthorised payment under the EFTA. See s. 909(a)(2) of the EFTA.

<sup>171</sup> The OCBC electronic service terms and conditions.

terminate the additional cardholder's authority. Though it is fair to make the consumer responsible for the transaction executed with the use of the additional card or/and PIN because he had consented to that use, requiring the consumer to return the card before the termination of the additional cardholder's is effective, may be unfair. In some circumstances, the consumer may face difficulty in taking control of the additional card from its holder. For example, the card may have been taken away by the cardholder without the consumer's consent. In this situation, it is impossible for the consumer to discharge the duty to return the card to the issuer.<sup>172</sup>

When the card is taken away, the issuer is, compared to the consumer, in a better position to manage the risk of the card being misused by the person who continues to possess the card though his authority has been terminated. For instance, the issuer can use a bulletin system, which is now widely employed in the electronic payment industries, to alert the merchant to the card's status when it contacted the issuer for payment authorisation.<sup>173</sup> Since the payment card has been upgraded to a PIN-based system, which means that authorisation is required for every single transaction irrespective of the amount,<sup>174</sup> the issuer may effectively use the bulletin to warn the respective merchants that the additional card has been cancelled.

---

<sup>172</sup> Clause 10.3 of the RHB, Clause. 6 of the OCBC, Clause 4.2 of the AmBank and Clause 21 of Maybank.

<sup>173</sup> For example clause 10.5 of the AmBank credit agreement and 10.5 of the RHB credit agreement provide that the issuer may place the number of the cancelled card on the Cancellation Bulletin for circulation to merchants and/or member banks of the credit card networks.

<sup>174</sup> The New England Debit Card Task Force, "Best Practice Guide for Managing Debit Card Fraud", 24th June 2005, at <<http://www.mecb.com/pdf/Best%20Practice%20Guide%20Final%207-17-05.pdf>>, at 2, (Visited 21st August 2005).

Among the contract terms reviewed, one term imposed even a harsher condition before the consumer's notice to terminate the additional cardholder's authority is effective. The RHB credit card terms and conditions provide:<sup>175</sup>

"...Cardmember shall continue to be bound by and liable under the terms and conditions of this agreement until the card...[is] received by RHB Bank Card Centre and duly cancelled..."

The above term can be used by the issuer to allocate to the consumer any unauthorised payment that has occurred after the card has been return to the issuer but before it was cancelled. By incorporating this clause, the issuer shifts the risk of fraud in distance transaction activities to the consumer.

This type of clause is detrimental to the consumer because it requires him to oversee that the issuer performed its responsibility to cancel the card. Since the risk of unauthorised use of the card is out of the consumer's control once the card is sent to the issuer, the losses should not be allocated to the consumer. After all, nobody can guarantee that an insider will not take the details from a card which has been cut and returned to the issuer and use them to initiate unauthorised payment or to give them to a third party.

(d) *Conclusive evidence clause*

A conclusive evidence clause is a clause which allows the issuer to present the record -

---

<sup>175</sup> Clause 2.6 of the RHB.



of the transaction and also of the proper functioning of the electronic payment systems security as proof of a valid payment mandate. This clause affects loss allocation because it imposes on the consumer a burden of rebutting the presumption that the payment was authorised. If the consumer failed to discharge this burden, he is liable for all the losses caused by the unauthorised payment as if the payment was validly made with his authorisation. In this situation, the consumer's liability can exceed the maximum limit which the issuer is allowed to allocate to the consumer under the respective electronic payment regulations.<sup>176</sup>

In Malaysia, the conclusive evidence clause is valid and enforceable as long as it satisfies the incorporation and the construction of contract rules. Accordingly, if the clause is part of the contract, and it is clear and unambiguous, the clause is as effective as any other term of the contract. To make the matter worse, in the case of a debit card payment, Para 14(4) (a) of the EFT Guidelines allows the issuer to prove the validity of the disputed payment by showing that the consumer's access code, or card or the EFT system was fully functioning on the day the payment was made, or that the issuer's employee or agents were not acting fraudulently or negligently in carrying out the EFT transaction.<sup>177</sup>

Hence, taking full advantage of this opportunity, to the detriment of the consumer, all-

---

<sup>176</sup> Section 133 TILA, s. 909 EFTA, s. 84 CCA, s. 12.12 Banking Code, Para 16 of the EFT Guidelines and Para 13 of the CC Guidelines.

<sup>177</sup> Clause 14(4)(a) and (b) of the EFT Guidelines.

sample EFT terms and conditions reviewed in this study contain clauses to that effect.

For example, clause 13 of the OCBC Electronic Services terms and conditions provides:

“The Bank’s records and any other records of instructions, operations or transactions made or performed, processed or effected through the Electronic Services by or purported to be by the Customer with or without his consent of any record of transactions relating to the operation of any Electronic Services and any record of any transaction maintained by any person equipped with terminals or by persons authorised by the Bank or any Relevant Person relating to the operation of any Electronic Services shall be binding and conclusive on the Customer for all purposes whatsoever and shall be conclusive evidence of the transaction and of the Customer’s liability to the Bank.”<sup>178</sup>

The conclusive evidence clause is certainly unfair as it creates an imbalance between the rights and obligations of both parties. In particular, the consumer is burdened with a difficult task of proving the unauthorised nature of the payment, while the issuer is given a right to refuse the disclosure of the technical details involved in an EFT transaction on security grounds.<sup>179</sup>

The conclusive evidence clause is used not only in the agreement for the debit card or EFT payment but also in the credit agreement. This practice clearly contradicts the CC Guidelines which required the issuer to prove that the payment was authorised before it can bind the consumer to it. Furthermore, by acting in contradiction of the CC Guidelines, the issuer commits an offence under s. 57 of the Payment Systems Act 2003. However, the continued presence of this type of clause in the issuers’ terms and conditions indicates the weaknesses of the CC Guidelines and also its implementing

---

<sup>178</sup> Clause 13 of the OCBC Electronic Services terms and conditions. Also and Clause 7 of the BCB PMPC-ATM Card terms and conditions and Clause 2 (i) of the BIMB Smart BIMB account terms and conditions. All on record with the researcher.

<sup>179</sup> See Para 28(a) of the EFT Guidelines.

statute in preventing the use of contract terms that affect the protection of the consumer against unauthorised credit card payment.

For instance, the RHB Bank terms and conditions provide:<sup>180</sup>

“RHB Bank shall be entitled to treat RHB Bank’s records of any transaction effected by the use of the Card including but not limited to transaction effected through the Internet or any other means acceptable to RHB Bank in its sole and absolute discretion from time to time, or by mail order or by telephone as evidence of a debt properly incurred by the Cardmember to be debited to the relevant Card Account notwithstanding that any such record may not contain any signature of the Cardmember.”

Other contract terms, like the Maybank’s and the Affin Bank’s<sup>181</sup> also give the issuers the right to rely on records of the transactions initiated by using credit cards, or card details as conclusive evidence of authorised payment.

All the above conclusive evidence clauses are substantively and procedurally unfair. Substantively, they are unfair because they allocate to the consumers losses beyond the maximum amount allowed by the CC and EFT Guidelines and treat an unauthorised payment as an authorised payment. Moreover, these clauses make the consumer powerless in protecting himself against unauthorised payment because they impose on him the burden to show that the payment was unauthorised. Considering consumer’s lack of access to the technical details of the issuers’ payment systems, and also the

---

<sup>180</sup> Clause 3.5 of the RHB Credit agreement terms and conditions. On file with the researcher

<sup>181</sup> Clause 6.10 of the AFFIN at <<http://www.affinbank.com.my/ccards/terms.htm#use>> and clause 14 of Maybank Gold credit card terms and conditions at <[http://www.maybank2u.com.my/consumeronline\\_card\\_s/agreement\\_gold.pdf](http://www.maybank2u.com.my/consumeronline_card_s/agreement_gold.pdf)>.

issuers' rights to maintain the confidentiality of related information, it is hard to imagine a situation where consumer can avoid liability for unauthorised payment.

Looking at the contract for electronic payment facilities which are standard form contracts, consumer does not really have the opportunity to refuse the incorporation of any of the contract terms including the conclusive evidence clause. In that situation, the presence of the consumer's signature on the contract documents does not really reflect his free consent to accept the conclusive evidence clause. As such, the above contract terms have failed in the procedural aspect of contract formation.

## **B      Comments on the Clauses from the Perspective of the Unfair Terms Rules in the United States and United Kingdom**

### *(a) Complex language and jargons*

The contract terms reviewed in this study were drafted using complex language and jargon that is hardly understood by the consumer. Although both the EFT and CC Guidelines require the terms and conditions of the contract for a credit card and EFT facilities to be written in plain and intelligible language, none of the terms and conditions referred to has this quality.<sup>182</sup>

---

<sup>182</sup> Paragraphs 6.2 of the EFT Guidelines and paragraph 6.1 of the CC Guidelines.

Since in Malaysia the common law rule of incorporation and construction of contract terms apply, the terms are enforceable and effective against the consumer, provided that they are successfully incorporated and not ambiguous. Therefore, it is hard for the consumer to challenge the enforceability of these terms when they are not invalidated by the CC and EFT Guidelines though they contradict their provisions.<sup>183</sup>

The main purpose of contract terms and conditions is to dictate the parties' duties and liabilities, including the consumer's potential liability for any unauthorised payment and his duty to maintain the security of his payment card and its associated PIN.<sup>184</sup> By using complex and difficult language, the consumer faces difficulty in understanding his duties and liabilities. As a result, it becomes impossible for him to fully perform his contractual duties, what is more to appreciate the consequence of his failure to discharge the duties.

If the reviewed terms are used by the issuers in the United States, they are not invalid simply because they are written using complex language. However, the consumer may challenge the enforceability of the ambiguous, long-winded contract terms on the grounds that it was not within his reasonable expectation because he did not have sufficient notice of the clauses or the clauses are illegible.<sup>185</sup> Because the procedural unconscionability rule renders an unconscionable term unenforceable, the issuer has to

---

<sup>183</sup> The issuer is liable to pay penalty for failure to comply with both Guidelines under s. 77 of the Payment Systems Act 2003. However, the terms remain effective.

<sup>184</sup> Para 6 of the EFT Guidelines.

<sup>185</sup> Section 211 (3) comment (f) of the Restatement (Second) of Contract 1981. *Wheeler v. St. Joseph Hospital* 133 Cal.Rptr. 775, 784, Cal.App. 1976 and *Allan v. Snow Summit, Inc.* 51 Cal.App.4th 1358, 59 Cal.Rptr.2d 813 Cal.App. 4 Dist., 1996. See also *Williston: A Treatise on the Law of Contract*, § 18:10, "Elements of unconscionability--Procedural and substantive unconscionability".

ensure that the terms which prescribe the consumer's duties and responsibilities are clear and legible.<sup>186</sup>

For example, in the case of *John Deere Leasing Co. v. Blubaugh*,<sup>187</sup> the court found the disputed terms which were stated on the back of the contractual document in fine, and light print to be nearly illegible. Indeed, the judge was forced to use a magnifying glass to read the disputed terms. Moreover, the wording was also found to be unreasonably complex. Therefore, it was decided that the disputed terms contained in an adhesive contract, buried and indecipherable, were procedurally unconscionable.

On the other hand, in the United Kingdom, Reg. 7 of the UTCCR requires the issuer to use "plain intelligible language" if the contract is in written form. When terms of a written contract are ambiguous, Reg. 7(2) requires the court to interpret the terms by using the *contra proferentum* rule. However, this rule only applies to a written contract, which ordinarily does not include an electronic contract.<sup>188</sup> Unless the definition of writing in Schedule 1 of the Interpretation Act 1978 is extended to include an electronic form of writing as suggested by the Law Commission<sup>189</sup> or Reg. 7 of the UTCCR is amended to include an electronic contract, this rule does not apply to an electronic

---

<sup>186</sup> Section 211 (3) of the Restatement (Second) of Contract 1981.

<sup>187</sup> 636 F.Supp. 1569 D.Kan., 1986. See also *Bank of Indiana, N.A. v. Holyfield*, 476 F.Supp. 104, 109-10 (S.D.Miss.1979), and *Wille v. Southwestern Bell*, 219 Kan. 755, 549 P.2d 903 Kan. 1976.

<sup>188</sup> Since the EU Directive on Unfair Terms in Consumer Contracts has no direct effect on individual in his or her relationship with anyone who is not a state or a machinery of state the consumer cannot use article 5.2 to protect itself in case the issuer used written contract terms which were not drafted in "plain, intelligible language". See Article 189 of the Rome Treaty 1957, which says to the effect that a Directive cannot be "directly applicable" to individual citizens of a Member State of the EU.

<sup>189</sup> Supra n. 81.

contract. Consequently, the limited scope of Reg. 7 may jeopardise consumer protection against unfair terms when the contract is electronically concluded.

The use of unintelligible language is one of the factors which the courts will consider in finding the fairness of a contract under the UTCCR. The honourable Bingham L. J in *Director General of Fair Trading v First National Bank*<sup>190</sup> emphasised: “The requirement of good faith in this context is one of fair and open dealing. Openness requires that the terms should be expressed fully, clearly and legibly, containing no concealed pitfalls or traps. Appropriate prominence should be given to terms which might operate disadvantageously to the customer. Fair dealing requires that a supplier should not, whether deliberately or unconsciously, take advantage of the consumer's necessity, indigence, lack of experience, unfamiliarity with the subject matter of the contract, weak bargaining position or any other factor listed in or analogous to those listed in Schedule 2 to the Regulations”.

The importance of intelligible language is shown by Reg. 6 of the UTCCR which requires all contract terms that contain the essence of the contract to be expressed in plain and intelligible language. Furthermore, the Office of Fair Trade guidance on unfair terms also shows that it treats contractual terms that are in small print or obscure wording, as contrary to good faith. The OFT also advised businesses against using

---

<sup>190</sup>[2002] 1 AC, 481, at 494, para 17. Followed by the case of *Picardi (t/a Picardi Architects) v Cuniberti* [2002] EWHC 2923, *Lovell Projects Ltd v Legg* [2003] B.L.R. 452 (QBD (TCC)), *Westminster Building Co Ltd v Beckingham* [2004] EWHC 138 and *Bryen & Langley Ltd v Boston* [2005] EWCA Civ 973.

jargon, complicated definitions, foreign words and phrases, and references to statutory provisions which are meaningless to most consumers.<sup>191</sup>

(b) *Exclusion and indemnity clause*

All exclusion and indemnity clauses reviewed in this study cannot be found in the contract terms used by the issuers in the United States. This is because s. 133 (d) of the TILA in the case of credit card payment and s. 909(e) of the EFTA in the case of debit card payment, prohibits the use of other liability rules which contradict their provisions unless the rule allocates a lesser liability to the consumers.

Even if the TILA and the EFTA do not prohibit the issuers from using exclusion and indemnity clauses that contradict their loss allocation rules, the reviewed clauses are unenforceable because they are in conflict with the public interest. In *Tunkl v Regent of the University of California*,<sup>192</sup> the court outlined the type of contract which contains an exculpatory or exclusion clause and the clause is unenforceable because it affects the public interest. The characteristics of the contract include:

(a) "It concerns a business of a type generally thought suitable for public regulation."

(b) "The party seeking exculpation is engaged in performing a service of great importance to the public, which is often a matter of practical necessity for some members of the public."

---

<sup>191</sup> Office of Fair Trade Bulletin No. 3 1997, at <<http://www.ofi.gov.uk/NR/rdonlyres/B11906BE-548C-46F5-9C8C-F602F8B9FE8E/0/ofi188.pdf>> (Visited 26th June 2006).

<sup>192</sup> 60 Cal.2d 92, at 99-101, 32 Cal.Rptr. 33, at 37-39, CAL. 1963.



(c) “The party holds himself out as willing to perform this service for any member of the public who seeks it, or at least for any member coming within certain established standards.”

(d) “As a result of the essential nature of the service, in the economic setting of the transaction, the party invoking exculpation possesses a decisive advantage of bargaining strength against any member of the public who seeks his services.”

All these characteristics are present in contracts for payment facilities. Thus, it is not ill-considered to suggest that if the reviewed exclusion and indemnity clauses were used in the United States they cannot be enforced against the consumers.

If the same clauses are used in a credit card agreement in the United Kingdom, they are also unenforceable because they contradict s. 173 of the CCA which renders any contract term that contradicts the CCA loss allocation rules void. On the other hand, if the clauses were used in a contract for a debit or charge card facility, it is likely that they are unenforceable because by using the clauses, the issuer breaches its promise to act fairly in dealing with the consumer.<sup>193</sup> This suggestion is coherent with the Ombudsman’s view that the Banking Code prevails over contract terms when they contradict each other in relation to a consumer’s liability for any unauthorised payment.<sup>194</sup>

---

<sup>193</sup> Section 2 and 6.2 of the Banking Code.

<sup>194</sup> Ombudsman News at <<http://www.financial-ombudsman.org.uk/publications/ombudsman-news/9/sept-disputed-cash-machine-withdrawals.htm>> (Visited 26th June 2006).

Other than being invalid for contradicting the CCA and the Banking Code, the enforceability of non-negotiable contract terms can also be examined by applying the UTCCR fairness test. If the terms are proven to have been inserted by an issuer who, according to Lord Bingham, “deliberately or unconsciously, take advantage of the consumer's necessity, indigence, lack of experience, and unfamiliarity with the subject matter of the contract, weak bargaining position or any other factor listed in or analogous to those listed in Schedule 2 to the Regulations,” they would fail the test.

Obviously, the exclusion and indemnity clauses reviewed in this study are in favour of the issuer as they shield the issuer against the risk of losses while exposing the consumer to the same risk. Furthermore, when the issuers inserted these terms in the contract, they failed to appreciate that some of the risks of an unauthorised payment cannot be avoided or prevented by the consumer either because the risk is outside his control or he does not possess the necessary resources, financially and intellectually to manage the risk.<sup>195</sup>

These exclusion and indemnity clauses may also be regarded as unreasonable from the UCTA perspectives because they allocate unauthorised payment losses to the consumer without distinguishing the losses caused by the consumer's fault, the issuer's fault and third party's fault.<sup>196</sup> Looking at the character of the electronic payment contract which is “a take it or leave it” standard form contract where the consumer is not given the

---

<sup>195</sup> See *Singer Co. (U.K.) Ltd. v. Tees and Hartlepool Port Authority* [1988] 2 Lloyd's Rep. 164 and *Flamar Interocean v Denmac (The Flamar Pride and The Flamar Progress)* [1990] 1 Lloyd's Rep. 434 and *Monarch Airlines Ltd v London Luton Airport* [1998] 1 Lloyd's Rep. 403,

<sup>196</sup> See above page 242-246.

opportunity to negotiate for more favourable terms, it is believed that all exclusion and indemnification clauses reviewed in this study are unreasonable.<sup>197</sup>

Furthermore, the clauses may also be unreasonable if their enforcement would injure the interests of the public.<sup>198</sup> Any contract term which allocates to the consumer unauthorised payment losses beyond the amount allowed by the CCA, the DSRs and the Banking Code contradicts these regulations, is inconsistent with public policy, and hence injures public interest.<sup>199</sup> As a result, the issuer cannot enforce the exclusion clauses and indemnity clauses against the consumer.

(c) *Onerous terms and conditions and conclusive evidence clause*

Clauses which describe the conditions for allocating unauthorised payment to the consumer are also onerous. In particular, the issuer's term which imposed on the consumer a strict duty to protect the secrecy of the PIN overlooked the inherent risk of a security failure of a publicly located terminal.

If these contract terms were used in the United States in a contract between an issuer of credit or debit card and a consumer, their enforcement can be challenged on the grounds of unconscionability. Procedural abuse is always found in an adhesive contract where

---

<sup>197</sup> *Phillips Products Ltd v Hyland* [1987] 2 All ER 620.

<sup>198</sup> See Steyn, J., "Fulfilling the Reasonable Expectations of Honest Man" and also *British Airports Authority plc v. British Airways Board* [1981] S. & B. AvR. 111/29, at 34 *per* Parker J who viewed that when the clause was allowed by the law it is not against public policy hence reasonable. Quoted in *Monarch Airlines Ltd. v. London Luton Airport Ltd.* [1998] 1 Lloyd's Rep. 403, at 406.

<sup>199</sup> Schedule 2 of the UCTA.

the parties have an unequal bargaining power. It is also possible to find the terms substantively unconscionable because the terms are in favour of the issuer. In particular, the terms do not reflect the multifaceted risk of unauthorised payment, which does not necessarily originate in the consumer's fault, and fail to allocate the risk according to the parties' ability to manage it.<sup>200</sup>

With regard to the notification clause, none of the credit agreements referred to contain clauses which require the consumer to give notice of unauthorised payment or possible unauthorised payment within a specific time frame because to do so would contradict the TILA, the CCA and the DSRs, respectively. Similarly, the EFTA also prohibits the use of contract terms that contradict its specific notification rules unless the contradictory terms provide better protection to the consumer.

In the United Kingdom, a review performed on several terms and conditions of the contract for a debit card facility showed that the issuers strictly follow the Banking Code which only require the consumer to give to the issuer notice of the event that may facilitate an unauthorised payment.<sup>201</sup> The Banking Code does not specify that the notice must be accompanied by a police report. To limit the protection of the consumer against unauthorised payment by the imposition of a duty to tender a police report is unfair as the notice given by the consumer demonstrates that sufficient steps have been

---

<sup>200</sup> *Goodwin v. Ford Motor Credit Co.*, 970 F. Supp. 1007 (M.D. Ala. 1997)

<sup>201</sup> Clause 5.4 of the HSBC First Direct Account Terms and Conditions, clause 2. of the First Trust Visa debit card Terms and Conditions, and clause 10.b of American Express Green Charge Card terms and Conditions at <[https://www66.americanexpress.com/eapp/uk/green/termsconditions\\_uk\\_green.jsp](https://www66.americanexpress.com/eapp/uk/green/termsconditions_uk_green.jsp)> (Visited 26<sup>th</sup> June 2006).

taken to inform the issuer of the potential risk. Thereafter, it is the issuer's duty to manage the risk. Hence, a contract term which requires the consumer to tender a police report before his loss can be limited is unfair under s. 5(1) of the UTCCR as it creates a significant imbalance in the rights and responsibilities of the parties.

Another term reviewed in this study imposed an unfair, burdensome responsibility on the consumer by allocating an unauthorised payment to him if he failed to return the payment card to the issuer. As argued beforehand, a notice to inform the issuer of the events which may facilitate an unauthorised payment should give sufficient information to enable the issuer to identify the payment card and the respective account under which it was issued. Acting on the information, the issuer can take appropriate action to prevent or reduce losses, which include circulating a warning against accepting the card to merchants. Hence, a failure to return the card does not affect the effectiveness of the loss preventive measure if the issuer has the proper technology to do so. Since the issuer possesses immense resources to innovate, develop and adopt the required technology, losses that occur after the notification had been made should not be allocated to the consumer despite his failure to return the card.

Another disturbing contract term is the term which imposes on the consumer the duty to oversee that the issuer performs its responsibility to cancel the payment card before the consumer is protected against unauthorised payment. It is believed that if this type of term was used in a contract for a credit card, charge card or debit card payment in the United Kingdom, it would be unfair, as it tilts in favour of the issuer. This unfair term

which would cause a significant imbalance in the rights and obligations of the consumer and the issuer, to the disadvantage of the consumer, would be unenforceable.<sup>202</sup>

If the contract term which requires the consumer to return the payment card to the issuer before he is protected against an unauthorised payment is used in a credit card agreement in the United States, the position is less clear because judicial decisions showed differences of opinions.<sup>203</sup> Nevertheless, in the interest of the consumer, it is best that the risk of a fraudulent payment which occurs after notice has been given to the issuer, but before the card was returned to it, should be managed by the issuer. The position is taken considering that the issuer has the required communication technology, such as a credit card warning bulletin, that allows it to display notice of cards' cancellation for reference by merchants.<sup>204</sup>

Regardless of the uncertain status of this type of contract term under the TILA, like other contract terms, its enforceability can be tested by applying the unconscionability test. Looking at the complexity of the language used in the reviewed term, a total disregard for the consumer's inability to manage the risk after the card was taken away without his consent, and the issuer's ability to warn merchants through specific communication systems against accepting the card, it is believed that the term is unfair and therefore unenforceable.

---

<sup>202</sup> *Director General of Fair Trading v First National Bank* [2002] 1 Lloyd's Rep. 489, *per* Bingham L.J. at para 17.

<sup>203</sup> See *Walker Bank & Trust Co. v. Jones*, 672 P.2d 73 (Utah 1983), cert. denied, 466 U.S. 937 (1984) and other cases discussed in chapter 3 on page 84 - 87.

<sup>204</sup> Mathews, M.E., "Credit Cards--Authorized and Unauthorized Use", at 287-291.

Finally, the discussion in Part A also looked into the effect of using a conclusive evidence clause. This clause affects the protection of the consumer against unauthorised payment because it imposes on him the duty to show that the issuer's record of the disputed payment was incorrect or the systems were not functioning properly at the time the disputed payment was initiated.

A review of several terms and conditions governing credit card and EFT payment facilities in the United States and the United Kingdom revealed that none of them contains a conclusive evidence clause.<sup>205</sup> The most obvious reason is because this clause undermines the provisions of the TILA, EFTA, CCA, Banking Code and also the DSRs which place the onus of proving authorised payment on the issuer.<sup>206</sup> Moreover, if the clause is used in the contract between a consumer and an issuer in the United States, the consumer may also challenge its validity by using the unconscionable contract rule.

In the United Kingdom, conclusive evidence clause may also fall under the category of an exclusion clause or a limitation of liability clause, depending on the extent of the protection against liability which it gives to the issuer. Accordingly, this clause must

---

<sup>205</sup> Natwest credit card terms and conditions at <<https://sol.natwest.com/creditcards/applyonline/ccardlegal.asp>>; Well Fargo credit card agreement at <[http://www.wellsfargo.com/credit\\_cards/select\\_card/secured/terms?\\_requee](http://www.wellsfargo.com/credit_cards/select_card/secured/terms?_requee)> Bank of America Fork at <[http://www.bankaf.com/about/disclosure\\_text.t.cfm#ee](http://www.bankaf.com/about/disclosure_text.t.cfm#ee)> (Visited 18th June 2006).

<sup>206</sup> Section 133 (b) of the TILA, s. 909 (b) of the EFTA, s. 171 (4) of the CCA, s.12.12 of the Banking Code. Even under the general law of banking, it is the duty of the issuer to show that the payment was authorised by the consumer.

satisfy the requirement of reasonableness before it can be enforced against the consumer.<sup>207</sup>

Section 13(1)(b) of the UCTA prohibits the use of contract terms that exclude or limit the consumer's rights or remedy against the issuer for the issuer's breach of contract or negligence<sup>208</sup> unless the clause is reasonable. Furthermore, s.13 (1) (c) also prohibits the use of any unreasonable term that restricts the rule of evidence or procedures. Furthermore, Schedule 2 para 1(q) of the UTCCR also indicates the possibility that this type of term defies good faith dealing. This is so because the term hinders the consumer from pursuing his right under the contract, limits his access to evidence; and imposes the burden of proving unauthorised payment on him, while the CCA, the DSRs and the Banking Code impose the onus of proving authorised payment to the issuer.

Finally, a conclusive evidence clause can also be unfair, according to the UTCCR rule as it was inserted by the issuer who exercised its superior bargaining power and took advantage of the consumer. Indeed, this clause has the effect of "unduly restricting the evidence available to [the consumer] or imposing on [the consumer] a burden of proof which, according to the applicable law, should lie with another party to the contract".<sup>209</sup>

---

<sup>207</sup> Section 13(1)(b) read together with s.2(2) and section s.3(1)(2)(a) UCTA.

<sup>208</sup> *Stewart Gill Ltd v Horatio Myer & Co.* [1992] Q. B. 600 and *Esso Petroleum Co. Ltd. v Milton* [1997] 1 W. L. R. 938.

<sup>209</sup> Regulation 5 of the UTCCR and Schedule 2 (q) of the UTCCR.



## 7 COMPARISON AND CONCLUSION

This chapter began with a review of the regulations of unfair contract terms applicable in Malaysia, the United Kingdom and the United States. It then analysed the contract terms used by the issuers in the contracts for electronic payment facilities.

Striking differences between the rules applicable in the three jurisdictions were identified in this review. In general, it discovered the weaknesses of the regulation of unfair terms in Malaysia in comparison to the position in the United Kingdom and the United States. More specifically, the review revealed the impact of the issuers' unfair terms on the protection of the consumer against unauthorised payment.

The first point that distinguishes the standard of protection against unfair terms in the three jurisdictions is the test used by the courts to determine the fairness of the disputed terms. As the tests varied, the results also varied, although the courts' common intention in applying the tests was to assess the enforceability of the relevant contract terms.

In the United States, the courts apply the common law rules of construction and incorporation of contract to determine the enforceability of contract terms. By applying these rules, the courts can determine whether the disputed term or terms have been successfully incorporated into the contract. Moreover, the courts can also use the rules to ascertain the scope of the disputed terms. In this way, the courts can discover whether the terms cover the matter which the consumer claims to be unenforceable.

Despite their merit, these rules are of limited application since they do not prohibit the use of unfair term *per se*. Accordingly, to improve the protection of contracting parties against unfair terms, a new rule was introduced. This rule, known as unconscionable contract rule, introduced the test of unconscionability of contract terms to be used by the courts to determine the enforceability of contract terms from the perspective of procedural and substantive fairness.

A similar approach was taken in the United Kingdom when the UCTA and the UTCCR were passed. The former questions the reasonableness of contract terms which fall under the category of an exemption clause only. The aim is to protect contracting parties against procedural and substantive unfairness. This can be understood by reading Schedule 2 of the UCTA which lists the circumstances which the courts may consider in examining the reasonableness of the disputed term. The UTCCR, on the other hand, allows the courts to question the enforceability of almost all the terms of the contract except the core terms which can only be challenged if they are not readily understood and written in unintelligible language.

These differences, however, may not exist for long if the Draft Bill prepared by the Law Commission is adopted as legislation because it propose a combined test of fairness and reasonableness of contract terms.<sup>210</sup>

---

<sup>210</sup> The Law Commission and the Scottish Law Commission Report on Unfair Terms in Contracts. Law Com; no. 292 and Scot Law Com; no. 199 Cm; 6464 at <[http://www.lawcom.gov.uk/docs/lc292\(1\).pdf](http://www.lawcom.gov.uk/docs/lc292(1).pdf)> (Visited 10th June 2006).

The above approaches, however, do not apply in Malaysia. The courts' power to assess the enforceability of contract terms is limited to applying the common law rule of construction and incorporation of contract terms. Accordingly, only the procedural aspect of the contract terms can be challenged i.e. whether the terms are part of the contract and whether the terms cover the disputed issue.

The second aspect that differentiates the unfair terms regulations in the three jurisdictions is the effect of the parties' unfair bargaining power in considering whether the terms meet the requirement of procedural fairness. In the United States, unequal bargaining power between parties, particularly between the consumer and the issuer who contracted via a standard form contract, may give rise to the finding of procedural unconscionability for lacking in negotiation and mutual consent.

Similarly, in the United Kingdom, the courts also examine the relative strength of the contracting parties' bargaining power to determine procedural fairness of the contract terms as indicated by the guidelines in Schedule 2 to the UCTA and the Grey List of the UTCCR.

In Malaysia, the court in *Wee Lian Construction* commented that unfair bargaining power should also be examined in considering the enforceability of contract terms. Nevertheless, because contract terms can only be challenged on the grounds of procedural fairness when they are part of an exclusion clause, the effect of using the

construction and incorporation rules is not as extensive as it should be if all the terms were subject to the test of procedural fairness.

The third element that distinguishes the regulation of unfair terms in the studied jurisdictions is the extent to which the courts are authorised to limit the contracting parties' freedom to contract.

Traditionally, a signed agreement binds the signatories, regardless of their actual knowledge of and consent to the terms of the agreement. Nevertheless, in the United States, judicial decisions showed that the courts have the authority to examine the validity of contract terms, regardless of the parties' signatures.

Meanwhile, in the United Kingdom, the courts also have jurisdiction under the UCTA and the UTCCR to scrutinise the fairness of terms used in a signed contract. Moreover, the courts' and the Ombudsman's decisions, and the list of potentially unfair terms published by the OFT showed that, terms in a signed agreement are not necessarily enforceable.

However, in Malaysia, special legal treatment is given to a signed agreement unless the party who disputed the contract term can show that his consent to the contract was obtained by fraud, misrepresentation, or undue influence or if he successfully pleaded *non est factum*. In case he failed to show a defective consent or that the document is not what he believed it was, a signed agreement is binding and enforceable, regardless of the

party's ignorance of its content. The law which recognises the theory of presumed consent to contract has a negative impact on the protection of the consumer against unfair terms, especially when the majority of contracts are reduced to a signed standard form contract, including a contract for electronic payment facilities.

Compared to the legal position in the United States and the United Kingdom, a combination of the freedom to contract theory and the Malaysian courts' lack of authority to question the substantive fairness of standard form contract terms, gives business entities the supremacy to exert control over the consumers to their advantage. This is evident in the reviewed terms and conditions discussed above.

In fact, the reviewed terms and conditions used by Malaysian issuers are injurious to consumers who use electronic payment facilities as the terms purported to reallocate losses caused by unauthorised payment transactions to the consumers in a very professional way. For instance, there is a term which was inserted with the aim to reverse the issuer's burden of proving the validity of the disputed payment to the consumer, hence forcing the latter to show that the payment was unauthorised to avoid losses. Another term indirectly allows the issuer to reallocate an unauthorised payment to the consumer by imposing on the consumer duties to prevent or reduce losses. Since the consumer may not be in a position to discharge the duties, his failure to prevent or reduce the losses may cause the losses to be allocated to him.

There is a two tier-test used to determine the enforceability of contract terms in the United States; at the first level, there are the common law rules of incorporation and construction of contract, and at the second level, the unconscionable contract rules, that allow the courts to thoroughly scrutinise the fairness of the contract terms. Similar observation can be made of the position in the United Kingdom because the UCTA, the UTCCR and s. 140A of the CCA 2007 authorise the courts to examine the fairness of the terms of the contract for electronic payment facilities. The legal approaches to the regulation of unfair terms in both the United States and United Kingdom are more effective in policing the use of unfair terms than the common law approach applied by the Malaysian courts.

Because a combination of the loss allocation rules for electronic payment systems and the unfair terms regulations implement a firm and strict regime of consumer protection against the unfair allocation of unauthorised payment, the issuers in the United States and United Kingdom are forced to be more prudent and fair in contracting with the consumers. This effect can be observed in the terms used in their contract terms which contain none of the unfair terms discussed in Part A. Compared to the terms used in the contract of the same nature in Malaysia, the terms used by the issuers in the United States and United Kingdom are more intelligible and understandable to the consumer. Moreover, simple, plain words and straightforward sentences are used instead of legal jargon.

Finally, in the United States and United Kingdom the protection of consumer against the use of unfair contract terms to allocate unauthorised payment is further strengthened by the provisions in the respective electronic payment systems' regulations which prohibit contracting out. These provisions render ineffective any term that contradicts their loss allocation rules, hence protecting the consumer against the issuer who might attempt to allocate the losses contrary to the respective regulations.

**1 SUMMARY**

The analysis in Chapter two to Chapter five considered various important aspects of the loss allocation rules in the electronic payment systems from the perspective of consumer protection. In the second and third chapters the discussion was focused on the allocation of unauthorised payment losses based on the mandate rules. Chapter four analysed the allocation of losses based on the consumer's receipt of benefit, and on his fraudulent conduct. That chapter also discussed the relationship between burden of proof and loss allocation. Finally, Chapter five discussed the regulations of unfair contract terms and their role in the protection of the consumer against the unfair contractual allocation of unauthorised payment losses.

**2 REVIEW AND RECOMMENDATIONS FOR REFORM**

The objective of this research was to analyse the rules which are applicable to the allocation of unauthorised payments in the electronic payment systems in Malaysia. The strategy was to compare the Malaysian rules with the rules that are enforced in the United States and United Kingdom for the same purpose. The aim was to identify the important elements of the loss allocation rules, to distinguish their strengths and weaknesses, and finally, to single out the elements that require improvement.



Applying the said strategy, three important aspects of the rules were identified as the elements which affect the protection of the Malaysian consumer against losses caused by unauthorised credit card and EFT payment. These elements are; the policy backgrounds, the substantive aspect of the loss allocation rules, and the implementation and enforcement of the rules.

#### **A      The Policy of Loss Allocation**

Apparently, neither the CC nor EFT Guidelines explained the underlying policy for their loss allocation rules. Hence, it is not clear whether the Guidelines are intended to protect the consumer or the issuer or to protect each of them against the fault of the other. In fact, it is possible that the failure of the Guidelines to prohibit contracting out indicates that they are not drafted with consumer protection in view.

Apart from that, since the implementation of the Guidelines is now covered by the Payment Systems Act 2003 which is intended to “promot[e] the reliable, efficient and smooth operation of the national payment and settlement systems and [to] ensur[e] that the national payment and settlement systems policy is directed to the advantage of Malaysia”, it is believed that the protection of the consumer is not a guiding principle in the formulation of the Guidelines’ loss allocation rules. Even if reference is made to the Banking and Financial Institution Act 1989, a statute under which the Guidelines were initially drafted, it indicated that the underlying policy of the Guidelines is more towards

regulating the business of banking and financial institutions rather than regulating the relationship between the customer and the banking and financial institutions.

As noted the lack of a specific policy background affects the formulation of the loss allocation rules. In particular, Chapter five, which discussed sample contract terms used in the contract between the consumer and the issuer of the credit card or debit card revealed the failure of the Guidelines, and also its implementing statute, the Payment Systems Act 2003, to protect the consumer against unfair loss allocation.

It is unfortunate that the Guidelines do not contain a clear underlying policy. A policy is important because it can provide assistance in the interpretation of ambiguous rules. Moreover, a policy is valuable when considering the applicability of the Guidelines to changes and developments that are taking place in the electronic payment systems such as the introduction of internet-based and mobile-based payment systems.

Therefore, it is believed that for there to be better and far reaching loss allocation rules, that are applicable to the changes that have happened and are still taking place in the electronic payment systems, and in particular, for the protection of the consumer against unfair loss allocation, the Guidelines should be reformed. This reform must be based on clear background policy. Hence, the first step to reform is to search for a suitable policy, taking into account the impact of unauthorised payment on the consumer, the advance of the consumer's development in terms of knowledge, the economy and social wellbeing, and finally, the impact of the loss allocation rules on society at large.

## **B Weakness in the Substance**

Besides having a clear underlying policy, the effectiveness of the loss allocation rules also requires clarity. Indeed, this is the element that is missing in some of the rules employed by the CC and EFT Guidelines.

### *(a) The scope of unauthorised payment*

The discussion revealed that the scope of any unauthorised credit card payment in the CC Guidelines is restricted to an unauthorised credit card payment that occurs as a consequence of loss or theft of the credit card. This narrow definition of unauthorised payment affects the consumer whose credit card is neither lost nor stolen but nonetheless who is a victim of an unauthorised payment initiated through the illegal use of his credit card details. Since distance payment via the telephone, an electronic banking facility or an internet commerce system could be initiated without presenting the card, the scope of an unauthorised payment leaves the issuer with the opportunity to allocate the losses caused by any unauthorised distance payment to the consumer via the contract terms.

As the risk of unauthorised distance payment is a contemporary risk faced by the consumer who participates in distance commerce activities, the rules in the CC Guidelines should be revised to incorporate a more general definition of an unauthorised payment.

It is indisputable that drafting rules that encompass all current and future modes of initiating credit card payment is not easy. Technology keeps evolving. The evolution may render obsolete what is today a clear and comprehensive rule. Therefore, the CC Guidelines should be revised by taking this into account and accordingly, they should incorporate a definition of an unauthorised payment that looks at the validity of the payment mandate and not at the method used to issue the mandate.

Nevertheless, the reform does not require much deviation from the existing definition. What should be done is to delete the part in the definition of an unauthorised credit card transaction that refers to the payment made as a “consequence of the lost or stolen card”. By abandoning this phrase, the definition will be broader and can cover all forms of unauthorised payment.

Furthermore, the CC Guidelines should also be reformed by adopting the TILA’s approach to impose on the issuer the duty to prove several pre-conditions before the losses can be allocated to the consumer. One of the TILA’s pre-conditions which is important in protecting the consumer against unauthorised payment, is the requirement that the issuer provides the consumer with a suitable identification method to determine the authority of the card’s user. This rule helps to protect the consumer against unauthorised payment when the credit card is used in any transaction where the technology employed does not facilitate identification of the person who initiated the payment.

With regard to the EFT Guidelines, the scope of an unauthorised payment is wider. Paragraphs 15 and 16 of the Guidelines clearly show that losses covered by the EFT Guidelines loss allocation rules do not have to be incurred as a consequence of the consumer losing control of the debit card either through loss or theft. As a matter of fact, the rules are applicable to losses caused by an unauthorised use of the consumer's access code which, in turn were caused by direct or indirect disclosure of the code to others or by a breach of the system's security.

Despite its merits, the EFT Guidelines' definition of an unauthorised payment also has a negative impact on the consumer. In this regard, Para 15 can be seen to imply allowing the issuer to allocate to the consumer the losses caused by an unauthorised payment when the payment was initiated using an unlawfully obtained access code or card details. For instance, the code or details might have been obtained by individuals who observed the consumer making his payment at a public payment facility such as an ATM or the merchant's terminal.

The said rule which allocates losses based on indirect disclosure of the code or the card details is unfair because it penalises the consumer for the fraudulent action of another over whom the consumer has no control. For example, when a consumer uses his debit card at a merchant's terminal, the employee who manages the terminal may collect the details for illegal purposes. Moreover, the rule is also prejudicial to the online consumer whose card details were observed by fraudsters who breached the payment system's security.

Furthermore, the loss allocation rules which allocate losses based on indirect disclosure of the code or card details is also inefficient because it imposes on the consumer liability for any unauthorised payment while he was not in a position to prevent the disclosure from taking place. Unless the payment industry can develop payment systems that can guarantee absolute confidentiality of the card details or the access code during a transaction, the scope of an unauthorised payment in the EFT Guidelines should be limited only to a payment initiated by using the details or code directly disclosed by the consumer to others.

*(b) Negligence and strict confidentiality as a basis of liability*

The EFT Guidelines determine the consumer's liability based on his failure to exercise reasonable care in protecting the access code security. Although the rule seems straight forward, its scope is not that easily understood. Therefore, it is believed that for the Guidelines to effectively encourage the consumer to exercise reasonable care in protecting his access code secrecy, they must demand the issuer to clearly stipulate in its contract terms the things which the consumer should or should avoid doing. This rule is akin to s 12.5 of the Banking Code 2005.

Other than negligence, the EFT Guidelines also allocate losses by looking at the consumer's failure to strictly maintain the confidentiality of the access code or the electronic devices used to effect the EFT payment. This rule affects the consumer in a system where the terminal is not totally secured from others' observation. In fact, the

reference in the EFT Guidelines to an electronic device which may include a computer or other devices located in public places such as a library, cyber café, one's office or university computer lab, may expose the consumer to unlimited losses. Hence, if the consumer's payment details which are stored in the device were to be obtained by a third party without his consent or knowledge, the consumer is responsible for the losses, according to the EFT Guidelines.

Based on the above observations, it is believed that the EFT Guidelines should be amended by abandoning the strict liability rule and at the same time, improving the negligence-based rule as suggested.

#### *(c) Notification rules*

The CC Guidelines do not contain a specific time frame for notification. This lack does not affect the protection of the consumer against unauthorised payment if the rule does not consider timely notification of the events that may facilitate an unauthorised payment as an important element of loss allocation.

Nevertheless, the CC Guidelines demand that the consumer should give notice of any potential unauthorised payment "as soon as reasonably practicable". This rule indicates that timely notification is important in the protection of the consumer against unauthorised payment.

In spite of the significant function of timely notification, the CC Guidelines' description of the notification period does not give to the consumer sufficient information to facilitate his process of making an *ex-ante* determination of the exact period of notification. The lack of information may prevent the consumer from effectively serving the issuer with the required notice to reduce or limit his losses. In this circumstance, the consumer will only know the status of his notification, either effective or ineffective to limit his losses, after his dispute with the issuer concerning the payment has been adjudicated.

This post-conflict supply of information is not in line with the disclosure approach to consumer protection which is supposed to address the problem of information asymmetry. In fact, a lack of concern with educating the consumer about the effect of an unauthorised payment and the steps necessary to prevent or reduce losses, indicates that the Guidelines were not primarily intended to provide protection against unauthorised payment to the consumer

The EFT Guidelines also require the consumer to inform the issuer of any potential unauthorised payment. However, Paras 14, 15 and 16 of the EFT Guidelines, which deal with unauthorised payment, do not specify the time frame for notification. As a result, the issuer is free to insert into its contract terms the period of notification which the consumer must comply with before the consumer's losses can be capped. This freedom of contracting produces various notification periods as discovered in the reviewed terms and conditions discussed in Chapter five.



Some issuers require the notice to be given immediately. However, it was also discovered how an issuer failed to insert a notification clause in its contract terms and conditions. By failing to specify the time frame for the notice of unauthorised payment to be given by the consumer, the issuer ignored the consumer's ability, in some circumstances, to act to protect himself against an unauthorised payment. While the consumer can avoid losses through the dissemination of information which he possesses, such as the loss or theft of his card, the issuer should have taken the opportunity to gather that information from the consumer as it benefits not only the consumer but also the issuer.

The lack of a clear and explicit notification rule in the EFT Guidelines and the different variation of the notification requirements in the contract terms and conditions used by the issuers are prejudicial to the interests of the consumer. These weaknesses affect the consumer because it makes the consumer who did not fully commit to reading the contract terms assume that all the terms are identical as the services are similar. Consequently, the consumer may not realise that the contracts terms of different issuers may stipulate a different period of notification.

Moreover, the ambiguity of the notification rule makes it difficult for the consumer to realise the importance of timely notification of the events that may lead to an unauthorised payment to him. In particular, he may not appreciate that the notice significantly affects the protection which he may enjoy against an unauthorised payment.

It is true that the issuer's cost of running the payment systems may increase as a result of the increase in the risk of loss that it has to bear. Hence, the rule which allows the consumer to give notice of a potential unauthorised payment anytime he wishes, like the one found in the TILA in the United States and in the CCA in the United Kingdom, will eventually be costly on the consumer because the issuer will try to spread the cost amongst the consumers. The issuer may do so in various ways including by increasing the service fees.

Notwithstanding the above impact of regulation, it is still possible to draft rules which are efficient and protective of the consumer but at the same time, which allow each party to bear a certain proportion of the cost. For example, the rule should specify with clarity the time frame for notification. This rule must facilitate the consumer's determination of the period of notification with ease. It should also describe the circumstances in which delayed notification will cause the losses to be reallocated from the issuer to the consumer and vice versa. In short, this form of notification rule should be modelled on s. 909 of the EFTA which described a different period of notification depending on the events which requires the notice to be given to the issuer.

*(d) Burden of proof*

In the cheque payment system and also in the general law of banking it is the duty of the bank to prove that the debit to the consumer's account was made with the consumer's authorisation. The same rule is adopted in the CC Guidelines and the EFT Guidelines.

Accordingly, when the consumer disputed credit card or EFT payment charged to his account the issuer must prove that the payment was authorised by the consumer. Failure to discharge this onus of proof means that all the losses are the issuer's except the amount of losses capped as the consumer's.

Irrespective of the advantage of the above rule, the EFT Guidelines contain another rule which jeopardises the protection of the consumer against unauthorised payment. Paragraph 14 of the EFT Guidelines allows the issuer to discharge the burden of proving authorised payment not only by bringing actual evidence of the consumer's mandate but also by bringing evidences of certain factual consideration which served as the basis for assuming that the payment was authorised.

The EFT Guidelines provide that evidences of a proper functioning of the consumer's access code or access device or the security of the payment systems are sufficient to prove the validity of the disputed payment. Accordingly, the consumer must to bring evidences to rebut this presumption. Otherwise, he will be responsible for the disputed payment.

This rule is unfair to the consumer because it imposes on him a duty to learn and understand the technical details of the overall systems, including the circumstances when the systems are properly or improperly functioning. Similarly, the rule also requires the consumer to learn the manner of the payment card and the access code

function. If he failed, it would be impossible for him to show that the access device or access code was not working when the disputed payment was made.

The rule affects the consumer severely as it imposes on the consumer the burden to learn about the technical details of the payment systems,. This is especially true as the issuer is given the right by the EFT Guidelines to refuse to disclose certain information about the payment systems if the disclosure will be a threat to the system's security. Since almost all information that explains the proper or improper functioning of the system is information about the technical details of the technology used in the payment systems, the issuer can easily protect itself against liability by refusing a disclosure. The issuer's refusal to supply the consumer with the information prevents the consumer from rebutting the presumption that the payment was authorised.

The above burden of proof rule is also limited in scope because it disregards the fact that proof of the proper functioning of the systems, the access code or access card does not necessarily mean that the payment made in a distance transaction was authorised. Since in a distance transaction a payment mandate is usually given by using the account or the card details, which can be obtained by a third party, without necessarily taking the card, this rule does not allow the consumer to bring other evidence to rebut the presumption that the payment was authorised. Additionally, the rule also reverses the burden of proof. Instead of the issuer bringing evidence to show that the payment was authorised, it now imposes on the consumer a duty to rebut the presumption of authority; a heavier

burden compared to the burden of defending himself against proof of authorisation by actual evidence of the mandate.

Therefore, it is believed that this rule should be deleted from the Guidelines. The issuer should be required instead to prove the authorised nature of the disputed payment by bringing evidence which shows the presence of a valid payment mandate made either by the consumer himself or by a person authorised by him.

*(e) Examination of the account statement*

Another aspect of the EFT Guidelines' loss allocation rules that may benefit the consumer if properly drafted is the rule which requires the consumer to examine the statement of account. Supposedly, this type of rule will require the consumer to check his account statement and thereafter, allocate the losses based on the consumer's compliance or non-compliance with the requirement.

This type of rule helps in reducing or preventing losses by asking the consumer to perform a duty which is within his capacity to perform. Since knowledge of an unauthorised payment or payments recorded in the statement can only be identified by the consumer, an examination of the statement is sufficient to alert the consumer to any suspicious transaction or transactions. He can verify the transaction or transactions and inform the issuer of the unauthorised nature of any of them. From then on, the responsibility to prevent or reduce unauthorised payment falls on the issuer.

Apparently, though, the EFT Guidelines require the consumer to check his account statement for unauthorised payment, it falls short of stipulating the penalty which the consumer will face for non-compliance. This flaw renders the rule futile as it only burdens the consumer with an obligation but fails to award the consumer for compliance or to penalise him for non-compliance.

In view of the above comments, the rule in the EFT Guidelines which requires the consumer to check his account statement must be amended. The purpose of the amendment is to create rules that encourage the consumer to act when he has the capacity to act to reduce or prevent losses and to reward or penalise him accordingly. Moreover, the new rule must explain in detail the manner in which the losses would be reallocated from the issuer to the consumer and vice versa.

*(f) Unfair terms regulations*

In Chapter five, it was shown that it is common to find that the contract for a credit card or debit card facility contains terms which contradict the CC or EFT Guidelines. The appalling attitude of the issuers, which do not have any regard to the protection of the consumer against the risk of unauthorised payment, is believed to be a tragic consequence of the failure of both Guidelines and their implementing statute, the Payment Systems Act, to strictly invalidate any contract term that contradicts the Guidelines' loss allocation rules.

The issuer's reliance on contractual loss allocation rules to allocate unauthorised payment losses to the consumer affects the consumer more severely since the merger of the financial and banking institutions in the late 90s and early 2000 reduced the number of electronic payment service providers.<sup>1</sup> Lack of competition may lead to conscious parallelism and a reduction in the number of competitive contract terms in the electronic payment industry. As a result, the consumer cannot practically shop around for a contract that allocates unauthorised payment losses on fairer terms and at the same time conforms to the Guidelines.

Although conscious parallelism is not a confirmed behaviour in a less competitive market, the consumer may still face difficulty in finding fairer terms. In particular, it is hard for the consumer to understand the meaning and scope of every term of the contract because of the complexity of the language used by the issuer. It was shown in Chapter five that it is common for the issuer's contract to use language and a style of writing that is legal in nature and contains much legal jargons that are hardly understood by an ordinary person.

Hence, to really understand the contract he intends to commit himself to, the consumer has to spend money and time to understand the contract terms. In most cases, because of time and financial constraints, the consumer blindly enters into a contract for electronic payment facilities. Furthermore, since a contract for electronic payment facilities are

---

<sup>1</sup> Central Bank of Malaysia Press Statement 29<sup>th</sup> July 1999 on "Merger Programme for Domestic Banking Institutions" at <<http://www.bnm.gov.my/index.php?ch=8&pg=14&ac=564>> (Visited 1<sup>st</sup> July 2006).

non negotiable, understanding the terms will not take the consumer anywhere in terms of negotiating for a fair allocation of unauthorised payment losses. As a result, the consumer will face the choice of having to accept the contract terms as they are or to avoid using the service; a tough choice to make, especially when current commercial activities require the service of electronic payment facilities.

The above problem is made worse by the lack of effective regulation of unfair contract terms in Malaysia. Because the common law rules of construction and incorporation of contract terms do not facilitate an *ex-ante* determination of the fairness of the respective contract terms, the consumer cannot be sure whether he is bound by the issuer's terms until the matter is decided by the Mediator or the courts.

The lack of unfair terms regulation means that the consumer representative body which is actively involved in consumer protection efforts cannot police the use of unfair terms on behalf of the consumer. More importantly, it cannot pressure the government agency that enforces the Guidelines and its implementing statute to forbid the use of any contract term on the grounds of unfairness because neither the general law of contract nor the Payment Systems Act renders a contract and /or its terms unenforceable on this basis.

It is apparent that the government's failure to regulate the use of unfair contract terms in Malaysia leaves the consumer in an uncertain position as to the enforceability of contract terms which allocate any unauthorised credit or debit card payment unfairly. This



uncertainty, together with the complexity of the language used in the contract, makes it impossible for the consumer to really exercise freedom to contract.

In view of the above weaknesses, two steps should be taken to improve the position of the consumer. First, it is necessary for both the EFT and CC Guidelines to be amended to insert a rule that prohibits contracting out. This rule would protect the consumer against the issuer who may try to unfairly allocate any unauthorised payment losses to the consumer.

Secondly, unfair terms regulations should also be introduced in Malaysia. The regulations general scheme of protecting the consumer against unfair contract terms will close any loopholes which the EFT and CC Guidelines may have. Consequently, the issuer will be prevented from taking advantage of the weaknesses of the Guidelines to unfairly burden the consumer with an unauthorised payment.

### **C Implementation and Enforcement Weaknesses**

As the names suggest, the EFT and CC Guidelines were purposely drafted to provide guidance to the issuers as to their rights and liabilities, and duties and responsibilities in their contractual relationships with the consumers. Because the Guidelines were not formulated as public regulations, the authority to enforce both Guidelines was given to the Central Bank of Malaysia (the “BNM”). Moreover, it also means that the consumer

cannot enforce the Guidelines in court. In fact, the implementation of the Guidelines is a matter of internal affairs between the payment systems providers and the BNM.

Successful implementation of any regulation requires the resolute and efficient exercise of power by the body assigned with the duty to administer and enforce the regulations. So far, it is not too extreme to suggest that the BNM has not been successful in forbidding the issuers of credit and debit card facilities against using contradictory loss allocation rules. In addition, it has also failed to sanction their violation of the Guidelines. These failures were discussed in Chapter five which showed the extensive use of contract terms that contradict the respective Guidelines.

The BNM's failure to implement the Guidelines is injurious to the protection of the consumers against unauthorised payment. Moreover, the enforcement failure also shows that a self-regulatory approach is not necessarily a suitable regulatory approach in all jurisdictions. In particular, self-regulation usually requires an active consumer movement with an influential pressure group that is capable of advancing the interests of the consumer. This pressure group must also actively be involved in monitoring industry non-compliance with respective regulation, and also in voicing the consumer's complaint and dissatisfaction with the enforcement of the regulations. The Malaysian consumer pressure groups are, however, not as strong and as active as the groups in the United States and United Kingdom. Hence, they are not very influential in representing consumers' interests.

Therefore, it can be concluded that when regulations are passed to govern the relationship between the consumer and businesses, successful enforcement of the regulations would require effective enforcement by the enforcing body. Furthermore, since the regulations affect society at large, it is also essential to subject the regulations to general public scrutiny by an effective independent body, free from any connection with the payment industry specifically, and the banking and financial institutions in general. To be successful, the efforts of these bodies should be given proper recognition and appropriate action should follow, depending on the circumstances of the case. Finally, the consumer should also be able to challenge the violation of the rules in court.

In view of the said weaknesses, and in the interest of the consumer, the state should interfere to regulate the relationship between the consumer and the issuer of the electronic payment facilities via state regulation. This regulation should contain a provision which is similar to the provisions of the TILA, the EFTA and the CCA that prevent contracting out. Moreover, the regulation should penalise issuers for contracting out by rendering the contradictory terms unenforceable. The prohibition and the penalty for non-compliance behaviour would force the issuers to allocate unauthorised payment losses in the manner described by the regulation.

Finally, the state should also regulate the use of unfair terms in a consumer contract. This regulation should be effective in monitoring the use of contract terms by businesses to their advantages and at the cost to the consumer. The regulation must contain provisions that can catch the issuers who may take advantage of any loophole in the

regulations that govern the electronic payment facilities to unfairly allocate unauthorised payment losses to the consumer.

## REFERENCES

### Books

1. Alsagoff, S A., Principles of the Law of Contract in Malaysia (1996) Malayan Law Journal.
2. Barron, R. G. and Jones, G., the Law of Restitution, 6th Edn.(2002) Sweet & Maxwell.
3. Beale, G. et. al. (Eds) Chitty on Contract, 29th Edn. (2004) Sweet & Maxwell.
4. Brindle, M. and Cox, R., Law of Bank Payments 3rd Edn. (2004) Sweet & Maxwell.
5. Calamari, D. and Perillo, J. M. The Law of Contracts, 3rd Edn. (1987) West Publishing.
6. Camp, L. J., Trust and Risk in Internet Commerce (2000) The MIT Press.
7. Cartwright, P., Banks, Consumers and Regulation, (2004) Hart Publishing.
8. Chalmer, J., *Evidence* (2006), Dundee University Press.
9. Chorafas, D. N., Electronic Funds Transfer (1988) Butterworth & Co (Publishers) Ltd.
10. Cranston, R., Principles of Banking Law 2nd Edn. (2002) Oxford University Press.
11. Davies, G., A History of Money From Ancient Times to the Present Day, 3rd Edn with revision (2002) University of Wales Press .
12. Ellinger, E. P., et al. (Eds), Modern Banking, 4th Edn.(2006) Oxford University Press.
13. Farnsworth, A., Contracts, 4th Edn. (2004) Aspen Publishers.
14. Fry, M. J. et al., Payment Systems in Global Perspective (1999) Routledge in cooperation with the Bank of England's Centre for Central Banking Studies.
15. Furmston, M. P. (Ed), Cheshire, Fifoot and Furmston's Law of Contract, 14th Edn. (2001) Butterworths.

16. Gloag, W. M., *The Law of Contract: a Treatise on the Principles of Contract in the Law of Scotland*, 2nd Edn. Reprint (1985) Caledonian Books.
17. Goode, R. M., *Consumer Credit Law and Practice* (1999) Butterworths.
18. Goode, R. M., *Commercial Law*, 3rd Edn (2004) Penguin.
19. Hance, O. and Balz, S. D., *The New Virtual Money: Law and Practice* (1999) Kluwer Law International.
20. Hapgood, M. (Ed), *Paget's Law of Banking*, 12th Edn. (2002) Butterworths Lexis Nexis.
21. Harvey, B. W. and Parry, D.L., *The Law of Consumer Protection and Fair Trading*, 5th Edn. (1996) Butterworths.
22. Hendry, M., *Smart Card Security and Applications*, 2nd Edn. (2001) Artech House.
23. Hingston, Q. A., *A Survey of Primitive Money: The beginnings of Currency* (1949) Methuen & Co. Ltd.
24. Holden, J. M., *The History of Negotiable Instruments in English Law* (1955) University of London The Anthlon Press.
25. Howells, G. G. and Weatherill, S., *Consumer Protection Law* 2nd Edn (2005) Ashgate.
26. Jevons, W. S., *Money and the Mechanism of Exchange*, 9th Edn (1890), K. Paul, Trench, Trübner.
27. Jones, G. (Ed), *Goff and Jones: The Law of Restitution*, 6th Edn.(2002) Sweet & Maxwell.
28. Lee, M. P., *Banking Law* (1995) Butterworths Asia.
29. Lawson R. G. *Exclusion Clause and Unfair Contract Terms*, 7<sup>th</sup> Edn (2003) Sweet & Maxwell.
30. Lewison, K., *The Interpretation of Contracts*, 3rd Edn. (2004) Sweet & Maxwell.
31. Lord, R. A. et al (Eds), *Williston: A Treatise on the Law of Contracts*, 4th Edn, (1990-2004) West Group.
32. Macdonald, E., *Exemption Clauses and Unfair Terms*, (1999) Butterworths.

33. Mann, R. J., Payment Systems and other Financial Transactions: Cases, Materials, and Problems, 2nd Edn. (2003) Aspen Law & Business.
34. McBryde, W. W., The Law of Contract in Scotland, 2nd Edn. (2001) W. Green.
35. Morris, D. "The Economics of Consumer Interest", in Morris, D., (Ed), Economics of Consumer Protection (1980) Heinemann Educational Books Ltd.
36. Nicholas, B., An Introduction to Roman Law, (1969) Clarendon Press.
37. O'Mahony, D., Peirce, M and Tewari, H., Electronic Payment System (1997) Artech House, Inc.
38. Pang, J., Banking and Finance in Malaysia (1995) Federal Publication Sdn Bhd.
39. Pearsall, J., The Concise Oxford Dictionary, 10th Edn. (2001) BCA.
40. Phang, A. B. L, Cheshire Fifoot and Furmston's Law of Contract, 2nd Edn. (1998) Butterworths Asia.
41. Proctor, C, Mann on the Legal Aspect of Money, 6th Edn. (2004) Clarendon.
42. Posner, R. A., Economic Analysis of Law, 6th Edn. (2003), 115, Aspen Publishers.
43. Reynolds, F.M.B., Bowstead and Reynolds on Agency, 18th Edn (2006), Sweet and Maxwell.
44. Sayer, E., Credit Cards and the Law: an Introduction, (1988) Format Publishing.
45. Scott, C. and Black, J. Cranston's Consumers and the Law 3rd Edn (2000) Butterworths.
46. Sinnadurai, V., The Law of Contract in Malaysia and Singapore: Cases and Commentary, 2nd Edn. (1987) Butterworths.
47. Vohrah, B. and Wu. M. A., The Commercial Law of Malaysia, 2nd Edn. (2003) Longman.
48. Walker, D. M., The Scottish Legal System: an Introduction to the Study of Scots Law 8th Edn (2001) W. Green/Sweet & Maxwell.
49. Walker, A. G., Law of Evidence in Scotland, 2<sup>nd</sup> Edn (2000), T & T Clark.
50. Zimmermann, R., The Law of Obligations: *Roman Foundations of the Civilian Tradition*, (1996), Oxford University Press.
51. Halsbury's Laws of England, 4th Edn Reissue 29 1(2)

## Articles

1. 2A Corpus Juris Secundum, Agency § 71
2. 3 Corpus Juris Secundum Agency § 513.
3. 42 Corpus Juris Secundum Implied Contracts § 29.
4. Alston, H. C., "Electronic Banking: Will That Be Cash, Credit, or E-money?" (1997) 1 *N.C. Banking Inst* 225 at 228.
5. Birks, P. and Chambers, R., "The Restitution Research Resource 1994" (1994) *R.L.R. Supp.* at vi-vii.
6. Birks, P., "'At the Expense of the Claimant': Direct and Indirect Enrichment in English Law", in D. Johnston and R. Zimmermann (Eds), *Unjustified Enrichment: Key Issues in Comparative Perspective*, (2002), at 505, Cambridge University Press.
7. Black, E. L., "Credit Card Debt As Nondischargeable Under Bankruptcy Code Provision Concerning Nondischargeability of Individual Debt Obtained Through False Pretenses, False Representation, or Actual Fraud, Other Than Statement Respecting Debtor's or Insider's Financial Condition", (2007) 158 *A.L.R. Fed.* 189.
8. Black, J., "Constitutionalising Self-Regulation" (1996) 59 *Modern Law Review* Issue 1, 24.
9. Brown, I., "The Significance of General and Special Authority in the Development of the Agent's External Authority in English Law", (2004) *J.B.L.* 391.
10. Burke, J. A., "Contract as Commodity: A Non-fiction Statutory Approach (2000) *Stat Law* 21(12).
11. Clark, M. S., Mills, J. and Powell, M. C., "Keeping Track of Needs in Communal and Exchange Relationships" *Journal of Personality and Social Psychology*, 51,2 (1986) 333-338.
12. Clark, S. C., "Walker Bank & Trust Co. v Jones: New Meaning for the Phrase 'Don't Leave without It'" (1984) *Utah L. Rev.* no. 4, 865.



13. Clarke, S. H., "Unmanageable Risks: Macpherson V. Buick and the Emergence of a Mass Consumer Market", (2005) 23 *Law & Hist. Rev.* 1.
14. Cooter R. D. and Rubin, E. L., "A Theory of Loss Allocation for Consumer Payments" (1987) 66 *Tex. L. Rev.* 63.
15. Crerar, L. D. "Banking, Money And Commercial Paper", *The Law of Scotland: Stair Memorial Encyclopaedia*, Reissue (2002)
16. Cross, M. L., "Husband's Liability to Third Person for Necessaries Furnished to Wife Separated from Him" 60 *A.L.R. 2d* 7. (2007) West Group.
17. Daughtrey, W. H. Jr. and Kidd, D. L. Jr , "Shifting Attorney's Fees In Litigation Attacking Commercial Arbitration Awards: A Disincentive For Meritless Motions For Correction, Modification or Vacatur", (1998) 35 *Am. Bus. L. J.* 515.
18. Doris, M. J., "Did We Lose The Baby With The Bath Water? The Late Scholastic Contribution to the Common Law of Contracts", (2005) 11 *Tex. Wesleyan L. Rev.* 361.
19. Ford, M. D., "Identity Authentication and 'E-Commerce'", 1998 (3) *The Journal of Information, Law and Technology (JILT)* at <http://elj.warwick.ac.uk/jilt/98-3/ford.html> (Visited 16th December, 2003).
20. Geva, B., "Allocation of Forged Cheque Losses - Comparative Aspects" *L.Q.R.* 1998, 114(Apr), 250.
21. Gillette, C. P., "Rules, Standard, and Precautions in Payment Systems" (1996) *Virginia Law Review* Vol. 82, 181, at 221-230.
22. Gobuty, D. E., "Defending Medical Information systems against Malicious Software" (2004) *International Congress Series* 1268, 96.
23. González, A. G., "PayPal: the Legal Status of C2C Payment Systems" (2004) *Computer Law & Security Report* Vol. 20 Issue 4, 266, at 297-298.
24. 37 *Am. Jur. 2d* "Fraud and Deceit", ss. 107-113.
25. Herzberg, A., "Payments and Banking with Mobile Personal Devices", *Communications of the ACM* (May 2003), Vol. 46 , Issue 5, at 53 – 58.
26. Howard, M., "Shifting Risk and Fixing Blame: The Vexing Problem of Credit Card Obligations in Bankruptcy", (2001) 75 *Am. Bankr. L.J.* 63.

27. Jackman, I. M., "Restitution for Wrongs", (1989) 48 *Cambridge L.J.* 302
28. Jung, B., et al, "Security Threat to the Internet: A Korean Multi-Industry Investigation" (2001) *Information & Management*, 38, 487-498.
29. Junseong, A., "Mobile Killer Applications In South Korea & Recommendations For U.S. Policymakers" (2003) 29 *Brook. J. Int'l L.* 239,
30. Kahn, C. M. and Roberds, W., "The Economic of Payment Finality", (2002) *Federal Reserve Bank of Atlanta Economic Review*, Issue 2, 1-12.
31. Keeton, R. E., "Insurance Law Rights at Variance with Policy Provisions", (1970) 83 *Harv. L. Rev.* 961.
32. Knapp, C. L., "A Tribute To Professor Joseph M. Perillo: Taking Contracts Private: The Quiet Revolution In Contract Law" (2002) 71 *Fordham L. Rev.* 761.
33. Kohlbach, M., "Making Sense of Electronic Money", (2004) No 1 *The Journal of Information, Law and Technology (JILT)* at<[http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004\\_1/kohlbach/](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_1/kohlbach/)>(Visited 10th March 2006).
34. Korobkin, R. B., "Bounded Rationality, Standard Form Contracts, and Unconscionability" (2003) 70 *U. Chi. L. Rev.* 1203.
35. Kronman, A. T., "Contract Law and Distributive Justice" (1980) the *Yale Law Journal*, Vol. 89, No. 3, at 472-511.
36. Kruk, T. L., "What constitutes violation of 18 U.S.C.A. § 1029, prohibiting fraud or related activity in connection with credit card or other credit access device" (2006) 115 *A.L.R. Fed.* 213.
37. Leff, A. A., "Unconscionability and the Code--The Emperor's New Clause", (1967) 115 *U. Pa. L. Rev.* 485.
38. Leming T. *et. al.*, "Purpose, construction, and application", 17 *Am. Jur. 2d*, Consumer Protection, §.3
39. Lepaulle, P., "The Function of Comparative Law: with a Critique of Sociological Jurisprudence" (1922) 35 *Harvard Law Review* 838.
40. Lundy, T., "Jury Instruction Corner", (2003) 27-*MAY Champion* 61.
41. Macdonald, E. and Poyton, D., "A Particular Problem for E-Commerce: Section 3 of the Unfair Contract Terms Act 1977" (2000) 3 *Web JCLI*, at

- <<http://webjcli.ncl.ac.uk/2000/issue3/macdonald3.html>> (Visited 25th Feb. 2005)
42. Macgregor, L. J., "Agency and Mandate" *The Law of Scotland*, Stair Memorial Encyclopaedia Reissue (2001) Law Society of Scotland/Butterworths.
  43. Mallat, N., "Theoretical Constructs of Mobile Payment Adoption" at <<http://w3.msi.vxu.se/users/per/IRIS27/iris27-1100.pdf>> IRIS (Information Systems research seminar in Scandinavia) conference paper no 27 Falkenberg, Sweden, 2004. (Visited 12th May 2006)
  44. Mallat, N., et al., "Mobile Banking Services", (2004) *Communications of the ACM* Vol. 47, Number 5, 42-46.
  45. Mather, H., "Restitution as a Remedy for Breach of Contract: The Case of the Partially Performing Seller" (1982) 92 *Yale L.J.* 14.
  46. Mathews, M. E., "Credit Cards--Authorized and Unauthorized Use" (1994) 13 *Ann. Rev. Banking L.* 233.
  47. Medvinsky, G. and Neuman, B. C., "NetCash: a design for practical electronic currency on the Internet", (1993) Proceedings of the 1st ACM conference on Computer and Communications Security.
  48. Melley, A. E. "Generally; express authority", and "Implied and Incidental Authority-Extent", 3 *Am. Jur. 2d*, Agency s 70 and s. 72.
  49. Melley, A. E. "Notice to third persons", 3 *Am. Jur. 2d*, Agency, s. 50.
  50. Miller, S. Smart Cards And Digital Cash, *The Law of Scotland: Stair Memorial Encyclopaedia*, Reissue (2002)
  51. Monestier, T. J., "'Nothing Comes of Nothing'. . . Or does It??? A Critical Re-Examination of the Doctrine of Separability in American Arbitration", (2001) 12 *Am. Rev. Int'l Arb.* 223.
  52. Petrylaite, R., "Can the Doctrine of Equitable Estoppel be applied against a Government?" (2004) *International Journal of Baltic Law*, Vol. 1 No. 2, 97-116.
  53. Pidgeon, A. C., "Show Me The Money" - But Don't Make Me Pay For It: An Analysis of Why Legislation Banning ATM Surcharges Is Inappropriate And Unwarranted, (1999/2000) 3 *N.Y.U. J. Legis. & Pub. Pol'y* 39.

54. Qing, S. and Wen, W., "A survey and Trends on Internet Worms", (2005) *Computers & Security* 24.
55. Rakoff, T. D., "Contracts of Adhesion: An Essay in Reconstruction" (1983) 96 *Harv. L. Rev.* 1174, at 1190.
56. Reed, C., "Consumer Electronic Banking" (1994) *J. I. B. L* 9(11) 451.
57. Reed, C., "What is a Signature?" 2000 (3) *Journal of Information, Law and Technology* ("JILT"). at <<http://elj.warwick.ac.uk/jilt/00-3/reed.html>> (visited 30th April, 2002).
58. Reilly, M. T., "The FDIC As Holder In Due Course: Some Law And Economics", (1992) *Colum. Bus. L. Rev.* 165.
59. Reynolds, F. M. B., "The Ultimate Apparent Authority" (1994) *L.Q.R.* 110, 21-25.
60. Rosenkranz, J., "The Pollution Exclusion Clause Through the Looking Glass", (1986) 74 *Geo. L.J.* 1237.
61. Rosmarin, W., "Consumers-R-Us: A Reality in the U.C.C. Article 2 Revision Process", (1994) 35 *Wm. & Mary L. Rev.* 1593.
62. Rougeau, V. D., "Rediscovering Usury: An Argument For Legal Controls On Credit Card Interest Rates" (1996) 67 *U. Colo. L. Rev.* 1.
63. Rubin, E. L., "Efficiency, Equity and the Proposed Revision of Articles 3 and 4", (1991) 42 *Ala. L. Rev.* 551.
64. Stempel, J. W., "A Better Approach to Arbitrability," (1991).65 *Tul. L. Rev.* 1377.
65. Stevenson, R. B., Jr., "The Regulation of Electronic Payment Systems: Ten Obvious Observations" (1998) *Glasser LegalWorks*, 117.
66. Tarasewich,, P. et al., "Issues In Mobile E-Commerce", (2002) *Communications of the Association for Information Systems*, Volume 8, at 41-64.
67. Weistart, J. C., "Consumer Protection in the Credit Card Industry: Federal Legislative Controls", (1972), 70 *Mich. L. Rev.* 1475.
68. Welling, S. N. and Rickman, A. G., "Cyberlaundering: the Risks, the Responses", (1998) 50 *Fla. L. Rev.* 295.

69. Whitty, N. R., Indirect Enrichment in Scots Law, (1994) *Judicial Review* 200.
70. Wigand, R. T., "Electronic Commerce: Definition, Theory, and Context", (1997) *The Information Society*, Vol. 13, NO. 1, 1-7
71. Williams, C. R., "Burdens and Standards in Civil Litigation" (2003) *Sydney Law Review* Vol. 25 No. 2, 165
72. Woodward, J. D., "Biometric Scanning, Law & Policy: Identifying the Concerns –Drafting the Biometrics Blueprint" (1997) 59 *U. Pitt. L. Rev.* 97.
73. Xavier, G., "Comparative Study of Arbitrations in Malaysia and Selected Jurisdictions in the European Union", [2002] 4 *MLJ* lxxxix.
74. Yong, Y. C., "Extending Mediation Practice to the Banking Industry", [2002] 3 *MLJ* cxc.
75. Zitter, J. M., "Necessity, In Action against Husband for Necessaries Furnished Wife, of Proving Husband's Failure to Provide Necessities" 19 *A.L.R.* 4th 432.
76. Department of Trade and Industry Unfair Contract Terms Bulletin (1997), No. 3.
77. The Law Commission and the Scottish Law Commission Report on, "Unfair Terms in Contracts" Cm 6464 February 2005.

### Internet References

1. Crasswell, R., Freedom of Contract, the Coase Lecture Series, at <[http://www.law.uchicago.edu/Lawecon/WkngPprs\\_26-50/33.Craswell.FrdmContract.pdf](http://www.law.uchicago.edu/Lawecon/WkngPprs_26-50/33.Craswell.FrdmContract.pdf)>(Visited 28th February 2006).
2. Central Bank of Malaysia Press Statement 29<sup>th</sup> July 1999 on "Merger Programme for Domestic Banking Institutions" at <<http://www.bnm.gov.my/index.php?ch=8&pg=14&ac=564>> (Visited 1<sup>st</sup> July 2006)
3. Felten, E W, et al., "Web Spoofing: An Internet Con Game" 20th National Information Systems Security Conference (Baltimore, Maryland), October, 1997,

- at <http://www.cs.princeton.edu/sip/pub/spoofing.pdf> (Visited 27th February, 2006).
4. Geva, B., "Consumer Protection in Electronic Funds Transfers", Research Paper for Industry Canada/ Office of Affairs (March 2002) at <http://www.osgoode.yorku.ca/gevapaper/gevaconspapermarch21.pdf> at 28, (Visited 20th March 2005).
  5. Hayashi, F. et al., A Guide to the ATM and Debit Card Industry, Federal Reserve Bank of Kansas City at <http://www.kc.frb.org/FRFS/ATMpaper.pdf> > at 1, (Visited 16th April 2006).
  6. Kubin, L., "Stanford E-mail Cracked", November 21 1993 in Suite 101.com at <http://www.suite101.com/article.cfm/hackers/12837> (Visited 27th March, 2003).
  7. McKitterick, D. and Dowling, J., "State of the Art Review of Mobile Payment Technovinskylogy" at 10-15, at <https://www.cs.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-24.pdf> (Visited 12th May 2006).
  8. Mesenbourg, T. L., "Measuring Electronic Business: Definitions, Underlying Concepts, and Measurement Plans" US Census Bureau, at <http://www.census.gov/epcd/www/ebusiness.htm> (Visited 11th January 2006).
  9. Singh, A. D., "Electronic Commerce: Some Implications for Firms and Workers in Developing Countries", (2000), at 10, The International Institute for Labour Studies Discussion Paper, at <http://www.ilo.org/public/english/bureau/inst/download/dp12300.pdf> (Visited 1st April 2006).
  10. Spangler, R., "Packet Sniffer Detection with AntiSniff", at <http://www.packetwatch.net/documents/papers/snifferdetection.pdf> (Visited 27th February 2006).

11. Wallace, J., et al., "Analysis of Market Circumstances Where Industry Self-regulation is Likely to be Most and Least Effective" at <<http://www.consumersonline.gov.au/downloads/selfreg/taskforce/ConsultantReport/ch1.pdf>> (Visited 20th December 2004).
12. Wu, J. and Lee, V., "Protection for Banking Consumers in the United Kingdom and The United States of America: Fees and Charges", December 2001 at <<http://www.legco.gov.hk/yr01-02/english/sec/library/0102rp01e.pdf>> (Visited 28th August 2005).
13. APACS Press Release 29th July 2005 at <<http://www.apacs.org.uk/>> (Visited 29th August 2005).
14. Australian Securities and Investments Commissions EFT Working Group, "Discussion Paper on an Expanded EFT Code of Conduct", (July 1999) at <[http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/fineft.pdf/\\$file/fineft.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/fineft.pdf/$file/fineft.pdf)> at 26 (Visited 20th March 2005).
15. Basel Committee on Banking Supervision Consultative Document on "Operational Risk" January 2001, at <<http://www.bis.org/publ/bcbzca07.pdf>> (Visited 26 April 2006).
16. Bank for International Settlement, Committee on Payment and Settlement Systems of the Group of Ten Countries, "Statistics on payment and settlement systems in selected countries", Figures for 2003, March 2005 at <<http://www.bis.org/publ/cpss66.pdf>> (Visited 16th April 2006)
17. Bank for International Settlement, Committee on Payment and Settlement Systems, "Clearing and Settlement Arrangements for Retail Payments in



Selected Countries, September 2000, at <http://www.bis.org/publ/cpss40.pdf> at 30, (Visited 26th August 2005).

18. Bank for International Settlements Committee on Payment and Settlement Systems, "Retail Payment in Selected Countries: A Comparative Studies" September 1999 at <http://www.bis.org/publ/cpss33.pdf> at 2-5 (Visited 10th December 2004).
19. Bank of England, "Payment Systems Oversight Report 2004", (January 2005) Issue 1 at <http://www.bankofengland.co.uk/publications/psor/psor2004.pdf>, at 7 (Visited 26th April 2006).
20. BBC News October 8 2002 "Fake bank website cons victims", at <http://news.bbc.co.uk/1/hi/technology/2308887.stm> (Visited 27th February 2006).
21. Boards of Governors of the Federal Reserve Systems Report to the Congress on the Disclosure of Point-of-Sale Debit Fees at <http://www.federalreserve.gov/boarddocs/rptcongress/posdebit2004.pdf> (Visited 10th March 2006).
22. Canadian Payments Association, Rule E2 Exchange for the Purpose of Clearing and Settlement Of Electronic On-Line Payment Items at [http://www.cdnpay.ca/rules/pdfs\\_rules/rule\\_e2.pdf](http://www.cdnpay.ca/rules/pdfs_rules/rule_e2.pdf) (Visited 10th April 2006).
23. DCMX mini™ offers by the NTT DoCoMo, Inc at <http://www.nttdocomo.com/pr/2006/001260.htmlVodafone-payment> (Visited 20th May 2006)
24. E-dinar at [http://www.e-dinar.com/html/3\\_2.html](http://www.e-dinar.com/html/3_2.html) (Visited on 26th April 2006).
25. Financial Mediation Bureau leaflet at [http://www.fmb.org.my/pdf/leaflet\\_eng](http://www.fmb.org.my/pdf/leaflet_eng).



- pdf*> (Visited 12th April 2006).
26. Financial Services and Technology Consortium, "What is eCheck?" at <http://www.echeck.org/overview/what.html> (visited 5th March 2003).
  27. Fox News "Security Breach May Put 40 Million Credit Card Holders at Risk" 18th June 2005 at <http://www.foxnews.com/story/0,2933,159943,00.html> (Visited 26th December 2005).
  28. "FSA Guide to Making a Complaint about Financial Services", at <http://www.fsa.gov.uk/consumer/pdfs/complaint.pdf> at 18, (Visited 10th of April 2005).
  29. Government of Australia Taskforce on Industry Self-Regulation, "Industry Self-Regulation in Consumer Markets" (2000), at 18 footnote 9, at [http://www.consumersonline.gov.au/content/selfregulation/finalreport\\_taskforce/03\\_chap2.asp](http://www.consumersonline.gov.au/content/selfregulation/finalreport_taskforce/03_chap2.asp) (Visited 20th December 2004).
  30. Institute for Communications Research Joint Project Feasibility Study "The Future Mobile Payments Infrastructure: A Common Platform for Secure M-Payments", <http://www.itu.int/ITU-D/pdf/4597-13.3bis-en.pdf> (Visited 10th April 2006).
  31. Internet Watchdog Warns of Fake eBay Web Site, The Mercury News, December 11th 2002 at <http://www.siliconvalley.com/mld/siliconvalley/news/4713932.htm> (Visited 27th March, 2003).
  32. MasterCard merchant.com "Authorization and Draft Capture: What Happens at the Point of Sale?" at [http://www.mastercardmerchant.com/build\\_business/pub](http://www.mastercardmerchant.com/build_business/pub)

*lic\_sector\_pointofsale.htm*> (Visited 10th April 2004).

33. MasterCard International News Release June 17, 2005, "MasterCard International Identifies Security Breach at CardSystems Solutions, A Third Party Processor of Payment Card Data" at <<http://www.mastercardinternational.com/cgi-bin/newsroom.cgi?id=1038>> (Visited 1st January 2006).
34. mPark payment services at <<https://www.mpark.com/mpark/memberReg.jsp>> (Visited 12th May 2006).
35. Nochex Online Payment at <<http://help.nochex.com/?Action=Q&ID=106>> (Visited 28th December 2005).
36. Nochex personal account agreement at <<http://help.nochex.com/messages/?Action=Q&ID=278>>, and merchant agreement at <<http://help.nochex.com/messages/?Action=Q&ID=271>> (Visited 10th April 2006).
37. Office of Fair Trade "Regulated and Exempt Agreement" June 2003 at <<http://www.offt.gov.uk/NR/rdonlyres/7BEE730B-3BA6-4F34-81E4-A046F78DB131/0/oft140.pdf>> at 3 and 6 (Visited 13th April 2005).
38. Osaifu-Keitai services also by NTT DoCoMo, Inc at <<http://www.nttdocomo.co.jp/english/service/imode/osaifu/index.html>> (Visited 26th April 2006).
39. Paypal, at <<http://www.Paypal.com>> (Visited 28th December 2005).
40. PayPal as an Additional Payment Option Technical Overview of at <[https://www.paypal.com/en\\_US/pdf/PP\\_Option\\_TechOverview.pdf](https://www.paypal.com/en_US/pdf/PP_Option_TechOverview.pdf)> (Visited 10th March 2006).
41. PayPal Mobile demonstration at <<https://www.paypal.com/cgi-bin/webscr?cmd=>

- xpt/mobile/MobileOverview-outside*> (Visited 11th April 2006).
42. PayPal Mobile payment at <<https://www.paypal.com/cgi-bin/webscr?cmd=xpt/cps/mobile/MobileFAQ-outside>> (Visited 12th May 2006).
  43. PayPal user agreement for United States at <<http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/ua-outside>> (Visited 10th April 2006).
  44. PayPal User Agreement for Europe at <<https://www.paypal.com/cgi-in/webscr?cmd=p/gen/ua/ua-outside>>(Visited 10th April 2006).
  45. The Financial Ombudsman News at <<http://www.financial-ombudsman.org.uk/publications/ombudsman.htm>> (Visited 12th June 2006).
  46. The New England Debit Card Task Force, “Best Practice Guide for Managing Debit Card Fraud”, 24th June 2005, at <<http://www.mecb.com/pdf/Best%20Practice%20Guide%20Final%207-17-05.pdf>>, at 2, (Visited 21st August 2005).
  47. The U.S. House of Representatives, Subcommittee on Domestic and International Monetary Policy, Committee on Banking and Financial Services, “The Future of Electronic Payments: Roadblocks and Emerging Practices”, at <[http://commdocs.house.gov/committees/bank/hba66988.000/hba66988\\_0.HTM#26](http://commdocs.house.gov/committees/bank/hba66988.000/hba66988_0.HTM#26)> (Visited 28th August 2005).
  48. Visa Media Center, News Release, San Francisco, 18 December 2002, at <<http://corporate.visa.com/mc/press/press128.html>> (visited 5 March 2003).
  49. Visa News Release, “Visa Global Debit Card Volume Surpasses Credit”, at <<http://www.corporate.visa.com/md/nr/press217.jsp>>, (Visited 29th August 2005).

50. "VisaNet: Delivering on the Promise of Secure and Reliable Payment" at <[http://www.visa.ca/en/about/mc\\_visanet.cf88.000/hba66988\\_0.HTM#26](http://www.visa.ca/en/about/mc_visanet.cf88.000/hba66988_0.HTM#26)> (Visited 28th August 2005).
51. WorldPay at <<http://www.worldpay.co.uk/>>(Visited 28th December 2005).
52. WorldPay merchant agreement at <[http://www.worldpay.com/about\\_us/index.php?Page=tandc](http://www.worldpay.com/about_us/index.php?Page=tandc)> (Visited 12th June 2006).
53. Yahoo Financial News, "MasterCard International Identifies Security Breach at CardSystems Solutions, A Third Party Processor of Payment Card Data" June 17th 2005, at <<http://biz.yahoo.com/bw/050617/175525.html?.v=1>> (Visited 5th March 2006)

#### Terms and conditions of the issuer's contract

1. Affin Bank Malaysia Credit Card Terms and Conditions at <<http://www.affinbank.com.my/ccards/terms.htm>> (Visited 20th June 2006)
2. American Express Charge Card terms and conditions clause 8 at <<http://www10.americanexpress.com/sif/cda/page/0,164,12004,00.asp>> (Visited 10th April 2006).
3. Barclays card terms and conditions at <[http://www.barclaycard.co.uk/Products/Apply/tandc/Student\\_graduate.html](http://www.barclaycard.co.uk/Products/Apply/tandc/Student_graduate.html)> (Visited 12th April 2006).
4. Citibank Malaysia Credit Card Agreement Terms and Conditions <<http://www>.

*citibank.com.my/APPS/portal/genericLoadPage.do?tabNo=3&htmlPageName=/info/det/creditcard\_tnc.htm*> (20th June 2006)

5. Cooperative Bank Current Account Terms and Conditions at <*http://www.cooperativebank.co.uk/servlet/Satellite?cid=1076405704423&pagename=CoopBank%2FPage%2FtplPageStandard&c=Page*> (Visited 12th June 2006).
6. HSBC Personal Banking Terms and Conditions at <*http://www.hsb.co.uk/1/PA\_1\_4\_24P/content/uk/pdfs/en/personal\_banking\_terms.pdf*> (Visited 12th June 2006).
7. Lloyds TSB Bank Credit Card at <*http://www.lloydstsb.com/media/lloydstsb2004/pdfs/AdvanceonlineTsCs.pdf*> (Visited 12th May 2006).
8. Maybank Gold Credit Card terms and conditions at <*http://www.maybank2u.com.my/con/consumer/online\_cards/agreement\_gold.pdf*> (Visited 20th June 2006).
9. RBS Student and Graduate Royalties Terms and Conditions at <*http://www.rbs.co.uk/Personal\_Finances/Students\_&\_Youth/Apply/sy\_terms.htm#d*> (Visited 12th May 2006).

## CREDIT CARD GUIDELINE

# **Credit Card Guideline**

Issued by:

Jabatan Sistem Pembayaran

Bank Negara Malaysia

18 March 2003

Version 1.0

## CONTENTS

Contents	Page
<b>PART ONE</b>	
1 Scope and effective date	1
2 Interpretation	1
<b>PART TWO</b>	
3 Minimum age and income requirements	2
4 Placement of fixed deposit	3
5 Prudent lending	3
6 Terms and conditions	4
7 Usage of credit card for unlawful activities	4
8 Minimum monthly repayment	4
9 Statement on minimum monthly repayment	5
10 Fees and charges	5
11 Minimum disclosure on fees and charges	6
12 Supplementary cardholder's liability	7
13 Liability for lost or stolen credit cards	7
14 Consumer awareness and education program	8
15 Suspension of interest on non-performing credit card loans and provision for bad and doubtful debts	8
16 Issuance of credit cards to directors	9
<b>PART THREE</b>	
17 Appointment of debt collection agencies	9
<b>Appendices</b>	
A Revoked circulars	10
B Statement on minimum monthly repayment	11
C Fees and charges table	13
D Suspension of interest on non-performing credit card loans and provision for bad and doubtful debts	14



## PART ONE

### **1. SCOPE AND EFFECTIVE DATE**

- 1.1 This Credit Card Guideline (Guideline) sets out the minimum requirements on credit card operations that shall be adhered to by all issuers of credit cards in Malaysia and is issued pursuant to sections 19 and 126 of the Banking and Financial Institutions Act 1989 (BAFIA). Any person who fails to comply with the Guideline may be guilty of an offence punishable under section 104 of the BAFIA.
- 1.2 With the issuance of this Guideline, all previous circulars on credit card operations as listed in **Appendix A** are revoked.
- 1.3 This Guideline shall come into force **immediately**, except for the following paragraphs which will come into force on **18 September 2003**:
- a. Paragraph 6;
  - b. Paragraph 7;
  - c. Paragraph 9;
  - d. Paragraph 11;
  - e. Paragraph 13; and
  - f. Paragraph 14.
- 1.4 **Part Three** of this Guideline shall only be applicable to issuers of credit cards who are licensed institutions.

### **2. INTERPRETATION**

- 2.1 In the Guideline, unless the context otherwise requires:
- 2.1.1 "Credit card" means a payment instrument that enables the cardholder to purchase goods and services or obtain cash against a line of credit, wherein the debt incurred may be settled

in full or in part on or before a specified date, and where the settlement is made in part, the balance may be subject to interest charges.

2.1.2 "Issuer of credit cards" means:

- a. A licensed institution that issues credit cards; or
- b. A person who has obtained Bank Negara Malaysia's (BNM) approval to issue credit cards under subsection 19(1)(b) of the BAFIA, and
  - i. the line of credit is provided by a licensed institution; or
  - ii. the issuance of the credit card is carried out through a joint venture arrangement with a licensed institution.

2.1.3 "Licensed institution" means any person licensed under subsection 6(4) of the BAFIA to carry on banking, finance company, merchant banking, discount house or money-broking business.

## **PART TWO**

### **3. MINIMUM AGE AND INCOME REQUIREMENTS**

3.1 An issuer of credit cards shall only issue credit cards to an applicant, as a principal cardholder, who is at least 21 years old and earning a minimum income of RM18,000 per annum<sup>1</sup>.

---

<sup>1</sup> Such requirements were previously in the circulars dated 24 December 1991 and 28 July 1999 listed in Appendix A.

#### **4. PLACEMENT OF FIXED DEPOSIT**

- 4.1 For an applicant who meets the minimum age requirement under paragraph 3.1 but is unable to prove his annual income, the issuer of credit cards shall require the applicant to place a fixed deposit of an amount equivalent to the approved credit limit to be granted to such applicant<sup>2</sup>.
- 4.2 An issuer of credit cards that is a non-licensed institution shall ensure that the applicant referred to in paragraph 4.1 shall place the fixed deposit with the licensed institution that is providing the line of credit or that is the joint venture partner of the issuer, as the case may be.

#### **5. PRUDENT LENDING**

- 5.1 An issuer of credit cards shall have an internal credit assessment policy for purposes of conducting a proper credit scoring exercise in approving or declining credit card applications and in determining an appropriate credit limit for each approved individual applicant.
- 5.2 An issuer of credit cards that is authorised to access the Central Credit Reference Information System (CCRIS) shall utilise the CCRIS and other sources of credit information for the purpose of verifying the applicant's credit worthiness to facilitate the credit assessment process.
- 5.3 An issuer of credit cards that is not authorised to access the CCRIS may, in addition to its internal credit assessment policy, rely on the licensed institution who is providing the line of credit or who is the joint venture partner of the issuer, as the case may be, for the purpose of verifying the applicant's credit worthiness to facilitate the credit assessment process.

---

<sup>2</sup> Such requirement was previously in the circular dated 21 January 1995 listed in Appendix A.

## **6. TERMS AND CONDITIONS**

- 6.1 An issuer of credit cards shall specify in the terms and conditions the significant liabilities and obligations applicable to the principal and supplementary cardholders in **bold print** in its application brochures and web pages. Such terms and conditions should be described in plain language, which is easily understood by the applicants.
- 6.2 An issuer of credit cards shall ensure that its customer service staff are able to answer queries on the credit card terms and conditions. The hotlines for the customer service shall be published in the brochures, monthly billing statements and web pages.

## **7. USAGE OF CREDIT CARD FOR UNLAWFUL ACTIVITIES**

- 7.1 An issuer of credit cards shall include in the terms and conditions under paragraph 6.1 a term specifying that the credit cards are not to be used for any unlawful activities such as illegal online betting. An issuer of credit cards shall immediately terminate the credit card facility if the cardholder is found to have used the credit card for an unlawful activity.

## **8. MINIMUM MONTHLY REPAYMENT**

- 8.1 An issuer of credit cards shall require their cardholders to make a minimum monthly repayment amount of 5% of the total outstanding balance<sup>3</sup>.

---

<sup>3</sup> Such requirement was previously in the circulars dated 24 December 1991, 7 November 1995, 2 January 1996, 11 September 1998 and 20 November 1998 listed in Appendix A.

## 9. STATEMENT ON MINIMUM MONTHLY REPAYMENT

- 9.1 An issuer of credit cards shall provide a statement, in the form as set out in **Appendix B**, on the **front page** of the monthly billing statement advising the cardholder on the consequences of paying only the minimum monthly repayment amount each month.
- 9.2 An issuer of credit cards shall provide the statement under paragraph 9.1 in Bahasa Malaysia if the monthly billing statement is published in a single language and in both Bahasa Malaysia and English if such statement is published in two languages.

## 10. FEES AND CHARGES

- 10.1 An issuer of credit cards, in imposing late payment charges and finance charges on their cardholders is subject to the following:
- a. A late payment charge may be imposed up to a maximum of 1% of the monthly repayment amount due or RM5, whichever is higher, if the cardholder fails to make the minimum monthly repayment by the due date<sup>4</sup>; and
  - b. A finance charge may be imposed up to a maximum of 1.5% per month which is equivalent to 18% per annum of the total outstanding balance<sup>5</sup>.
- 10.2 All retail transactions (as opposed to cash advance transactions) charged to a credit card shall be allowed an interest free period of at least 20 days from the posting date of such transaction, regardless of the total outstanding balance in the credit card account. In this regard, the finance charge (interest) shall only be charged on the balance that remains outstanding in the account from the preceding monthly billing statement date, which shall be calculated on a daily basis. In other

<sup>4</sup> Such requirement was previously in the circular dated 30 December 1998 listed in Appendix A

<sup>5</sup> Such requirement was previously in the circular dated 30 December 1998 listed in Appendix A

words, all retail transactions posted to the account after the previous statement date shall not be included in the total outstanding balance for the purpose of computing the finance charges. Finance charges shall not be clawed back to the date when the transaction has been posted to the cardholder's account and shall only be computed commencing from the due date following the interest free period<sup>6</sup>.

## **11. MINIMUM DISCLOSURE ON FEES AND CHARGES**

- 11.1 An issuer of credit cards shall specify the credit card fees and charges in a readily understandable manner to the applicant, using concise language and in a table as provided in the standard format in **Appendix C** ('Fees and Charges Table').
- 11.2 An issuer of credit cards shall ensure that the Fees and Charges Table is placed prominently and noticeably on the credit card application forms including electronic application forms, preferably on the same page of such forms. If otherwise, a conspicuous reference to the disclosure shall be indicated in the application forms. In the case of electronic application forms, the issuer of credit cards shall ensure that the Fees and Charges Table is brought to the notice of the applicant in such manner that the applicant cannot bypass such Fees and Charges Table before the applicant submits his credit card application.
- 11.3 An issuer of credit cards shall print on the **front page** of the monthly billing statement to cardholders, information on the various charges (including finance charges) imposed on the outstanding balances and the method of computation of such charges. The effective interest rate charged on credit card accounts shall be printed on the basis of 'per

---

<sup>6</sup> Such requirement was previously in the circulars dated 7 November 1995 listed in Appendix A.



annum'. The issuer of credit cards is allowed to also print the interest rate on a daily or monthly basis in addition to the 'per annum' basis<sup>7</sup>.

## **12. SUPPLEMENTARY CARDHOLDER'S LIABILITY**

- 12.1 An issuer of credit cards shall not hold the supplementary cardholder jointly or severally liable for the debts of the principal cardholder or other supplementary cardholders.

## **13. LIABILITY FOR LOST OR STOLEN CREDIT CARDS**

- 13.1 An issuer of credit cards shall provide effective and convenient means by which a cardholder can notify any lost, stolen or unauthorised use of his credit card and shall provide procedures for acknowledging receipt and verification of the notification for the lost, stolen or unauthorised use of credit card.
- 13.2 The cardholder's maximum liability for unauthorised transactions as a consequence of a lost or stolen credit card shall be confined to a limit specified by the issuer of credit cards, which shall **not exceed RM250**, provided the cardholder has not acted fraudulently or has not failed to inform the issuer of credit cards as soon as reasonably practicable after having found that his credit card is lost or stolen.
- 13.3 Where the amount imposed on to the cardholder for unauthorised transactions due to lost or stolen credit cards is in excess of the maximum liability limit, the issuer of credit cards has to prove that the cardholder has acted fraudulently or failed to inform the issuer of credit cards as soon as reasonably practicable after having found that his credit card is lost or stolen.

---

<sup>7</sup> Such requirements were previously in the circulars dated 7 November 1995 and 2 January 1996 listed in Appendix A.

13.4 An issuer of credit cards shall ensure that the cardholders shall not be held liable for any unauthorised transaction charged to the credit cards after they have notified the issuer of credit cards verbally or in writing, that their credit cards are lost or stolen. An issuer of credit cards shall take immediate action upon notification by the cardholder, to prevent further use of the lost or stolen credit card.

13.5 An issuer of credit cards shall notify the cardholders in the monthly billing statements of the cardholders' potential liability for unauthorised transactions if they have acted fraudulently or have failed to inform the issuer of credit cards as soon as reasonably practicable upon discovery that their credit cards have been lost or stolen.

#### **14. CONSUMER AWARENESS AND EDUCATION PROGRAM**

14.1 An issuer of credit cards shall conduct a consumer awareness and education program on a continuing basis which shall include:

- a. Advice on "comparison shopping" for credit cards;
- b. Advice on prudent use of credit cards;
- c. Consequences of paying only the minimum monthly repayment amount;
- d. Advice on fraud prevention measures; and
- e. Potential liability for lost or stolen credit cards.

#### **15. SUSPENSION OF INTEREST ON NON-PERFORMING CREDIT CARD LOANS AND PROVISION FOR BAD AND DOUBTFUL DEBTS**

15.1 An issuer of credit cards who is a licensed institution shall comply with the "Guidelines on the Suspension of Interest on Non-Performing Loans and Provision for Bad and Doubtful Debts" issued by BNM which may be revised from time to time.



- 15.2 An issuer of credit cards who is a non-licensed institution shall ensure that the suspension of interest on non-performing credit card loans and provision for bad and doubtful debts comply with the requirements as specified in **Appendix D**.

## **16. ISSUANCE OF CREDIT CARDS TO DIRECTORS**

- 16.1 Pursuant to subsection 62(1) of the BAFIA, exemption is given to licensed institutions to issue credit cards to their directors, provided that the licensed institutions ensure that the credit card shall be utilised as a charge card<sup>8</sup>.
- 16.2 An issuer of credit cards who is a non-licensed institution shall ensure that the credit cards issued to their directors shall be utilised as a charge card.
- 16.3 An issuer of credit cards shall ensure that all transactions charged to the credit cards issued under paragraph 16.1 and 16.2 above are settled by the cardholders before or on the payment due date and the cardholders are not allowed to have any outstanding balance in their credit card accounts after the payment due date.

## **PART THREE**

## **17. APPOINTMENT OF DEBT COLLECTION AGENCIES**

- 17.1 An issuer of credit cards who is a licensed institution may outsource the debt collection functions with regard to its **credit card receivables** in accordance with the circulars entitled 'Appointment of Debt Collection Agencies by Banking Institutions' and 'Outsourcing of Banking Operations' issued by BNM which may be revised from time to time.

---

<sup>8</sup> Such requirement was previously in the circular dated 18 July 1996 listed in Appendix A.

**APPENDIX A – Revoked Circulars**

<b>NO.</b>	<b>CIRCULAR</b>	<b>ISSUE DATE</b>
1	Guidelines on Credit Card Operations	24 Dec 1991
2	Credit Card with Line-Of-Credit to Fixed Depositors (Ref: 2201/808/26/3/HY/SAH/MAH)	21 Jan 1995
3	Guidelines on Credit Card Operations (Ref: 2201/808/26/3/HY/SAH/MAH)	7 Nov 1995
4	Guidelines on Credit Card Operations (Ref: 2201/808/26/3/HY/SAH/MAH)	2 Jan 1996
5	Issuance of Credit Cards to Directors (Ref: 2201/808/26/3/RMI/SAH)	18 Jul 1996
6	Bayaran Minimum Bulanan Bagi Kad Kredit (Ref: JSP/POL/4110/CF/JM)	11 Sep 1998
7	Bayaran Minimum Bulanan Bagi Kad Kredit	20 Nov 1998
8	Garispanduan Mengenai Operasi Kad Kredit	30 Dec 1998
9	Minimum Income for Credit Cards (Ref: JSP/POL/4109/5)	28 Jul 1999

## APPENDIX B – Statement on Minimum Monthly Repayment

### Notis Jika Hanya Membayar Bayaran Minimum Bulanan:

Jumlah faedah yang harus dibayar dan tempoh yang diambil untuk menjelaskan keseluruhan baki belum jelas anda akan bertambah jika anda hanya membayar bayaran minimum bulanan. Berikut adalah gambaran jumlah faedah yang dikenakan dan tempoh pembayaran balik, bagi senario-senario baki belum jelas yang berbeza jika anda hanya membayar bayaran minimum secara berterusan. Pengiraan adalah berdasarkan 5% bayaran minimum atau RM\_\_\_\*, yang mana lebih tinggi, pada caj kewangan sebanyak \_\_\_\*% setahun.

### Notice on Paying Only Minimum Monthly Repayment:

*The amount of interest you have to pay and the time it takes to repay your balance in full will increase if only the minimum monthly payment is made. The following table illustrates the amount of interest incurred and the repayment period, under different outstanding amount scenarios if you continue to pay only the minimum amount. The computations are based on 5% minimum payment or RM\_\_\_\*, whichever is higher, at a finance charges of \_\_\_\* % p.a.*

	<b>Contoh bagi senario-senario baki belum jelas yang berbeza/ Examples under different outstanding amount scenarios</b>					
Baki belum jelas/ Outstanding balance (RM)	500	1,000	1,500	2,000	5,000	10,000
Tempoh pembayaran balik/ Repayment period (bulan/ months)	*	*	*	*	*	*
Jumlah faedah yang dikenakan/ Total interest incurred (RM)	*	*	*	*	*	*

**Note:** \* Figures to be provided by the issuer of credit cards, based on their rates & charges.

Where there are space constraints, an issuer of credit cards is allowed to disclose part of the statement on the front page of the monthly billing statement, and to disclose the remainder of the statement at the back of the monthly billing statement with a clear reference made to it, as follows:

Front Page of Monthly Billing Statement

**Notis Jika Hanya Membayar Bayaran Minimum Bulanan:**  
Jumlah faedah yang harus dibayar dan tempoh yang diambil untuk menjelaskan keseluruhan baki belum jelas anda akan bertambah jika anda hanya membayar bayaran minimum bulanan. Sila rujuk kepada perkara \_\_\_\_ di muka surat belakang untuk maklumat lanjut.

**Notice on Paying Only Minimum Monthly Repayment:**  
*The amount of interest you have to pay and the time it takes to repay your balance in full will increase if only the minimum monthly payment is made. Please refer to item \_\_\_\_ at the back page for details.*

Back Page of Monthly Billing Statement

**Notis Jika Hanya Membayar Bayaran Minimum Bulanan:**  
Berikut adalah gambaran jumlah faedah yang dikenakan dan tempoh pembayaran balik, bagi senario-senario baki belum jelas yang berbeza jika anda hanya membayar bayaran minimum secara berterusan. Pengiraan adalah berdasarkan 5% bayaran minimum atau RM \_\_\*, yang mana lebih tinggi, pada caj kewangan sebanyak \_\_\*% setahun.

**Notice on Paying Only Minimum Monthly Repayment:**  
*The following table illustrates the amount of interest incurred and the repayment period, under different outstanding amount scenarios if you continue to pay only the minimum amount. The computations are based on 5% minimum payment or RM \_\_\*, whichever is higher, at a finance charges of \_\_\* % p.a.*

	Contoh bagi senario-senario baki belum jelas yang berbeza/ Examples under different outstanding amount scenarios					
Baki belum jelas/ Outstanding balance (RM)	500	1,000	1,500	2,000	5,000	10,000
Tempoh pembayaran balik/ Repayment period (bulan/ months)	*	*	*	*	*	*
Jumlah faedah yang dikenakan/ Total interest incurred (RM)	*	*	*	*	*	*

**Note:** \* Figures to be provided by the issuer of credit cards, based on their rates and charges.

## APPENDIX C – Fees and Charges Table

An issuer of credit cards shall adopt the following Fees and Charges Table which shall be printed using a minimum of 8-font size (the table is shown in a 8-font size):

Fees and charges*																									
a) Annual fee: i) Principal ii) Supplementary	<div>The annual fees are :</div> <table><tr><th rowspan="2">Card Type</th><th colspan="2">VISA (RM)</th><th colspan="2">MasterCard (RM)</th></tr><tr><th>Principal</th><th>Suppl.</th><th>Principal</th><th>Suppl.</th></tr><tr><td>Classic/ Standard</td><td></td><td></td><td></td><td></td></tr><tr><td>Gold</td><td></td><td></td><td></td><td></td></tr><tr><td>Platinum/ Premier</td><td></td><td></td><td></td><td></td></tr></table>	Card Type	VISA (RM)		MasterCard (RM)		Principal	Suppl.	Principal	Suppl.	Classic/ Standard					Gold					Platinum/ Premier				
Card Type	VISA (RM)		MasterCard (RM)																						
	Principal	Suppl.	Principal	Suppl.																					
Classic/ Standard																									
Gold																									
Platinum/ Premier																									
b) Joining fee	<div>The fees are :</div> <div>i) Supplementary RM____ iii) Gold RM____</div> <div>ii) Classic/Standard RM____ iv) Platinum/Premier RM____</div>																								
c) Finance charges: i) Purchases ii) Cash advance iii) Balance transfer	<div>The charges are :</div> <div>i) ____% p.a. of the outstanding amount calculated on a daily basis.</div> <div>ii) ____% p.a. of the cash advance amount calculated on a daily basis.</div> <div>iii) ____% p.a. of the amount transferred calculated on a daily basis.</div>																								
d) Cash advance fees	The cash advance fee is ____% of the amount advanced or a minimum of RM____, whichever is higher. This is imposed for each cash advance transaction.																								
e) Minimum monthly repayment	5% of the outstanding balance or a minimum of RM____.																								
f) Late payment charge	The late payment charge is ____% of the minimum repayment amount due or a minimum of RM5, whichever is higher. [To include other related charges, if any]																								
g) Interest free period	____ days from the date of the monthly billing statement and only applicable for purchase transactions.																								
h) Conversion for overseas transactions	The conversion rate as determined by Visa International or MasterCard International plus administration cost of ____%.																								
Note : For promotional offers, an issuer of credit cards is required to mention the duration of the promotion period, i.e. start and end date, and the conditions that apply, if any.																									

## APPENDIX D – Suspension of Interest on Non-Performing Credit Card Loans and Provision for Bad and Doubtful Debts

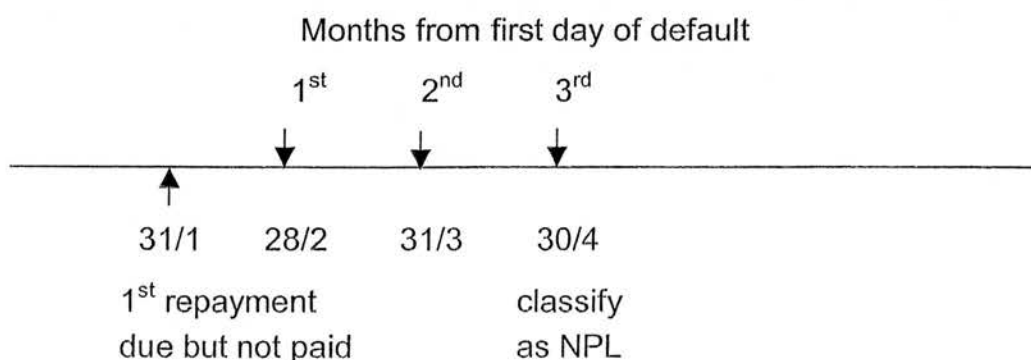
### Introduction

1. The objective of the requirement is to establish minimum standards on the classification of non-performing credit card loans and provision for bad and doubtful debts, income recognition and loss provisioning by issuers of credit cards who are non-licensed institutions so that there is a realistic valuation of loan assets and prudent recognition of income.

### Classification of Non-Performing Credit Card Loans

#### Classification of credit card accounts as non-performing credit card loans

2. A credit card account is classified as a non-performing loan when the cardholder fails to settle his minimum monthly repayments for 3 months or more from the first day of default. This is illustrated as follows:



#### Treatment of partial repayments of credit card loans

3. For purposes of ascertaining the period in arrears, each minimum monthly repayment must be made in full. If the cardholder settles his minimum monthly repayment partially, the repayment is still deemed to be in arrears.



## **Treatment of interest and penalty interest on non-performing credit card loans**

4. All interest accrued from the date the credit card account is classified as non-performing shall forthwith be suspended and credited into the "interest-in-suspense" account. Interest suspended should be credited to the "interest-in-suspense" account and reflected in the accounts of the issuer of credit cards. Memorandum entry is permitted only when the credit card account has been fully or partially written off.
5. An issuer of credit cards is required to claw-back interest to the first day of default. In this regard, interest accrued and recognised as income prior to the date the credit card account is classified as non-performing must be reversed out of income. Suspension of interest on a non-performing credit card account will commence from the date the credit card account is classified as non-performing. Subsequently, interest earned on a non-performing credit card account will be recognised as income on a cash basis i.e. only when the interest is received by the issuer of credit cards.
6. Penalty interest should be treated in the same manner as normal interest. Similarly, penalty interest should be recorded in the books of credit card accounts and not maintained as a memorandum entry.

## **Reclassification of non-performing credit card loans as performing**

7. A non-performing credit card loan can be reclassified as performing once total instalment in arrears falls below 3 months. For example, if a credit card loan is 4 months in arrears and the cardholder pays 2 monthly instalments, the non-performing credit card loan can be reclassified as performing as the total period in arrears is below 3 months. When the credit card loan is reclassified as performing, interest can be recognised as income on an accrual basis. If the loan remains at all times below 3 months in arrears, the loan can be

classified as performing and interest income can be recognised or accrued accordingly.

### Provisions for Bad and Doubtful Debts

8. An issuer of credit cards is required to review the adequacy of the general and specific provisions for bad and doubtful debts at all times to ensure that the provisions set aside are reflective of their potential losses.
9. In respect of specific provisions, an issuer of credit cards is required to observe the following minimum parameters:

Period of Default	Classification	<i>Minimum specific provision over the amount outstanding, net of unearned interest and interest suspended</i>
3 months but less than 6 months	Doubtful	50% provisioning
6 months and above	Bad	100% provisioning

10. Notwithstanding the above, an issuer of credit cards should be further guided by the general principles enumerated below for purposes of determining the level of provisioning required:

(i) **Doubtful accounts**

Credit facilities or a portion thereof where collection in full is **improbable** and there is a high risk of **ultimate default**.

(ii) **Bad accounts**

Credit facilities or a portion thereof which are deemed **uncollectible and worthless**, on the basis of relevant circumstances.



## **Other issues**

### **Issuing of new credit cards for a non-performing credit card account**

11. Where an issuer of credit cards issues a credit card and the account of the credit card subsequently is classified non-performing, the same issuer of credit cards or other institutions in the same group, as the case may be, is not allowed to issue a new credit card to the defaulting cardholder to settle the arrears.

### **Write-off on non-performing credit card loans**

12. Credit card accounts or portions thereof which are classified as bad or deemed uncollectible and worthless should be written-off. To ensure that the health of the issuer of credit cards is not distorted by writing off the credit card accounts which are deemed still collectible as a guise to suppress the true level of non-performing credit card loans and interest-in-suspense, it shall be the management's responsibility to ensure that prudent and proper monitoring of credit card accounts is enforced.
13. Before a credit card account can be written off, the issuer of credit cards should seek the approval of the Board of Directors or the management committee, as the case may be.

### **Write-back of specific provision**

14. Write-back of specific provision is permitted under the following circumstances:-
  - (i) where the credit card account has been fully settled;
  - (ii) where there is cash inflow; or
  - (iii) where there is concrete evidence to support a reclassification of the credit card account to a better category.

## **Minimum requirement**

15. Issuers of credit cards may adopt more stringent measures in addition to the minimum requirements mentioned in this **Appendix D**.

## Guidelines on Consumer Protection on Electronic Funds Transfers

## **GUIDELINES ON CONSUMER PROTECTION ON ELECTRONIC FUND TRANSFERS**

### **PART I**

#### **PRELIMINARY**

##### **Scope and Interpretation**

1. The purpose of these Guidelines is to provide a basic framework to establish the rights, liabilities and responsibilities of customers and financial institutions relating to electronic fund transfers.
2. These Guidelines are issued pursuant to sections 119 and 126 of the Banking and Financial Institutions Act 1989.

##### **Definitions**

3. For purposes of these Guidelines -

"Access code" includes pin, password or code which provides a means of access to a customer's account for the purposes of initiating an electronic fund transfer;

"Account" means any account maintained with a financial institution;

"Beneficiary" means the person named in a payment order who is to be paid by the beneficiary bank;

"Beneficiary bank" means the bank identified in a payment order which is to make payment to a beneficiary -

- (a) by crediting the account of beneficiary; or
- (b) in any other manner, where the payment order does not provide for crediting an account;

"Card" means any card, including an ATM card, EFTPOS card, debit card, credit card or stored value card, used by a customer to effect an electronic fund transfer;

"Customer" means a natural person using an electronic fund transfers facility provided by a financial institution;

"Financial institution" means a financial institution licensed under section 6(4) of the Banking and Financial Institutions Act 1989;

"Payment order" means a payment instruction by a customer to a financial institution, transmitted orally, electronically, or in writing, to pay, or to cause another financial institution to pay, a fixed or determinable amount of money to a beneficiary.

## **PART II**

### **SCOPE OF ELECTRONIC FUND TRANSFER**

#### **Coverage of electronic fund transfer**

4. For purposes of these Guidelines, electronic fund transfer means fund transfers carried out through or by means of:

- (a) telegraphic transfer;
- (b) point-of-sale terminal;
- (c) stored value card terminal;
- (d) cash dispensing machine;
- (e) cash deposit machine;
- (f) telephonic instruments; or
- (g) debit card.

#### **Exceptions to electronic fund transfer**

5. The term "electronic fund transfer" in paragraph 4, does not include -

- (a) any cheque or authorisation service which does not directly result in a debit or credit to a customer's account; or
- (b) any automatic transfer from a savings account to a current account and vice versa pursuant to an agreement between a customer and a financial institution.

**PART III**  
**TERMS AND CONDITIONS**  
**FOR ELECTRONIC FUND TRANSFER**

**Terms and Conditions**

6.(1) A financial institution providing any type of electronic fund transfer shall have standard terms and conditions in relation to the carrying out of electronic fund transfers.

(2) The standard terms and conditions shall be in writing in the National Language and English, in clear, readily understandable and user friendly manner.

(3) The standard terms and conditions shall be disclosed by a financial institution to a customer before or at the time the electronic fund transfer is carried out.

(4) The standard terms and conditions shall include -

- (a) the customer's liability for any unauthorised electronic fund transfer and duty to report to the financial institution promptly any loss, misuse, theft or unauthorised use of, access code or a card;
- (b) the telephone number and address of the department in charge of electronic fund transfers of the financial institution to be notified in the event the customer believes that an unauthorised electronic fund transfer has been or may be effected;
- (c) the customer's right to stop payment of a preauthorised electronic fund transfer and the conditions and procedures to initiate such stop payment order;
- (d) information relating to lodgement of complaints, investigation and resolution procedures;
- (e) the customer's right to receive relevant documents in relation to electronic fund transfers; and
- (f) the circumstances where the financial institution may in the ordinary course of business, disclose information in relation to customer's affairs or account to a third person.

(5) The instruction of a customer to stop payment of a preauthorised electronic funds transfer as mentioned under subparagraph (4)(c) shall operate immediately unless agreed otherwise by the customer and financial institution whereby a date or time is predetermined.

(6) For the purposes of this paragraph, "preauthorised electronic fund transfer" means any prior arrangement or agreement between a customer and a financial institution to authorise the financial institution to -

- (a) make payments to a third party out of the funds standing in the account of the customer; or
- (b) transfer funds from one account of the customer to another account of the customer maintained with the financial institution or another financial institution.

#### **Availability of the terms and conditions**

7. A financial institution shall make available copies of the standard terms and conditions at its branches that provide electronic fund transfer services.

#### **Changes in the terms and conditions**

8. A financial institution may vary or modify the standard terms and conditions of an electronic fund transfer in relation to -

- (a) imposing or increasing charges;
- (b) increasing the customer's liability for losses; or
- (c) adjusting the transaction limits on the use of a card,

provided it gives 30 days prior written notice to the customer.

#### **Notification of other changes**

9.(1) A financial institution may notify the customer of any other changes in the standard terms and conditions through -

- (a) notice in the periodic statement of account;
- (b) notice at ATM, EFTPOS or other electronic terminals;

- (c) notice at its branches; or
- (d) any other mode it deems suitable.

(2) Where notification is given under subparagraph 9(1)(b), (c) or (d) and the customer is not notified directly, subsequent written advice shall be provided to the customer by the financial institution.

### **Exception to notification**

10. Notwithstanding paragraph 9, advance notice need not be given when changes are necessitated by an immediate need to restore or maintain the security of an electronic fund transfer, an electronic fund transfer system or an individual account.

### **Consolidation of changes**

11. Where important or a sufficient number of changes so warrant, a financial institution may issue a single document providing a consolidation of variations made to the standard terms and conditions.

### **Charges**

12. A financial institution may impose charges on a customer who uses an electronic fund transfer, in accordance with its rules on tariff and charges.

## **PART IV**

### **TELEGRAPHIC TRANSFER**

#### **Duties of financial institution**

13.(1) A financial institution shall transmit a telegraphic transfer, within the same working day the customer makes the request or application for the telegraphic transfer.

(2) A financial institution shall not be liable for the failure to carry out its obligations under subparagraph (1) if the customer has insufficient funds in his account to effect the transfer.



(3) A financial institution has a duty to execute a payment order on the same working day the payment order is received from another financial institution.

(4) The beneficiary bank shall notify the beneficiary as soon as possible provided the customer has given sufficient information.

(5) A beneficiary bank shall not impose any charges for expenses incurred in notifying the beneficiary of a payment order.

## **PART V**

### **ERRONEOUS AND UNAUTHORISED ELECTRONIC FUND TRANSFER**

#### **Duty to notify errors**

14.(1) A customer shall notify his financial institution of any error in his statement of account or possible unauthorised transaction in relation to his card or access code.

(2) The notification shall be made in writing within 60 days from the date of the statement of account.

(3) Where there is a complaint of an unauthorised electronic fund transfer by a customer, the burden of proof is on the financial institution to show that the electronic fund transfer was authorised.

(4) The burden of proof in subparagraph (3) shall be satisfied if the financial institution proves that -

- (a) the access code, card and the security of the fund transfer system was fully functional on that day; and
- (b) the officers of or agents appointed by, the financial institution were not fraudulent or negligent in carrying out the electronic fund transfer.

(5) For the purposes of this paragraph, error in statement of account includes -

- (a) an incorrect electronic fund transfer to or from the customer's account;  
or
- (b) an addition or omission in the periodic statement of an electronic fund transfer affecting the customer's account.

**Duties of customer**

15.(1) A customer shall not -

- (a) directly or indirectly disclose to any person the access code of his card or any electronic device used to effect an electronic fund transfer; or
- (b) fail to take reasonable care to keep the access code secret.

(2) A financial institution is discharged from any liability if it is proven that the customer has breached the duty imposed by subparagraph (1).

(3) A customer shall not be liable for losses resulting from an unauthorised transaction occurring after he has notified the financial institution that his card has been lost, misused, stolen or that the access code security has been breached.

**Delay in notification**

16. Where the customer has contributed to a loss resulting from an unauthorised transaction by, delaying notification of, lost, misused or theft of the card, or someone else knowing the access code of the card, the customer is liable for the actual loss which occurred, except for -

- (a) that portion of the loss incurred on any one day which exceeds the daily transaction limit applicable to the card or account; or
- (b) that portion of the total loss incurred which exceeds the amount of funds standing in the customer's account.

**Circumstances where customer is not liable**

17.(1) A customer shall not be liable for loss -

- (a) not attributable to or not contributed by the customer;
- (b) caused by the fraudulent or negligent conduct of officers of or agents appointed by, the -
  - (i) financial institution;
  - (ii) companies and other financial institutions involved in networking arrangements within this country; or

- (iii) merchants who are linked to the card system;
- (c) relating to a card that is forged, faulty, expired or cancelled; or
- (d) occurring before the customer has received his card or access code.

(2) Where any dispute arises in relation to a customer's card, it is to be presumed that the customer did not receive the card, unless the financial institution can prove otherwise.

## **PART VI**

### **DUTIES OF FINANCIAL INSTITUTION**

#### **Notification of loss, theft or unauthorised use of card**

18. A financial institution shall provide an effective and convenient means by which a customer can notify any loss, misuse, theft or unauthorised use of a card or breach of access of security.

#### **Procedures for acknowledging notification**

19.(1) A financial institution shall provide procedures for acknowledging receipt of notifications, including telephone notification, by a customer for any loss, misuse, theft or unauthorised use of a card or breach of access code security.

(2) The acknowledgement need not be in writing provided the financial institution has a means by which a customer can verify that he had made a notification and when such notification was made.

#### **Liability in cases of system or equipment malfunction**

20.(1) A financial institution shall be liable to its customer -

- (a) for a loss caused by the failure of an electronic fund transfer system or equipment to complete a transaction accepted by a terminal, in accordance with the customer's instruction; or

- (b) for computing or book keeping error made by the financial institution.
- (2) A financial institution shall inform a customer immediately through -
  - (a) notice at ATM, EFTPOS or other electronic terminals;
  - (b) notice at its branches; or
  - (c) any other mode it deems suitable.

if it is aware that the system or equipment to carry out electronic fund transfer is not available for use or where there is a malfunction.

(3) Where the customer should have been aware that the system or equipment was not available for use or malfunctioning, the financial institution's responsibilities are limited to the correction of any error in the customer's account, and the refund of any charges or fees imposed on the customer for that transaction.

#### **Liability in a case of act of God**

21. Notwithstanding paragraph 20, a financial institution shall not be liable to its customer if the failure to carry out an electronic fund transfer was caused by or resulted from an act of God or other circumstances beyond its control, provided the financial institution had exercised reasonable care and diligence.

#### **Security of deposits at electronic terminal**

22. The security of a deposit received at an electronic terminal shall be the responsibility of the financial institution receiving the deposit, from the time the transaction is completed, subject to verification of amount deposited.

#### **Discrepancy between money deposited and recorded**

23. Where there is a discrepancy between the amount recorded as having been deposited at an electronic terminal and the amount recorded as having been received, the financial institution shall notify the customer of the difference on the next working day and shall advise the actual amount which has been credited to the customer's account.

**Shared arrangements**

24. A financial institution shall not avoid any obligation to its customer by reason only of the fact that it is a party to a shared electronic fund transfer system, and that another party to the system had failed to fulfil its obligations under these Guidelines.

**PART VII****INVESTIGATION AND RESOLUTION PROCEDURE****Complaints and Investigation**

25.(1) A financial institution shall -

- (a) establish formalised procedures for the lodgement of complaints by customers of matters covered by these Guidelines;
- (b) establish appropriate procedures for the investigation and resolution of any complaint by a customer; and
- (c) set out in standard terms and conditions the means and procedures to lodge a complaint.

(2) A customer is required to disclose to the financial institution all relevant information relating to the complaint except his access code.

(3) The financial institution shall, as far as possible, settle all complaints immediately.

(4) The financial institution's decision in relation to a complaint is to be made on the basis of all relevant established facts and not on the basis of inferences unsupported by evidence.

**Extension of time to settle complaint**

26.(1) Where a financial institution is unable to settle a complaint immediately as required under paragraph 25(3), it shall inform the customer immediately for the need of 14 days to resolve the complaint.

(2) Where a financial institution is unable to resolve the complaint within 14 days, it shall notify the customer in writing of the need for an extension of time which shall not in any case exceed 30 days from the date the complaint is lodged.

(3) A financial institution shall promptly advise the customer of the outcome of the investigation, together with reasons for the outcome upon completion of its investigation.

**Incorrectly credited or debited account**

27. Where as a result of the investigation of a complaint, a financial institution discovers that the customer's account has been incorrectly credited or debited, the financial institution where appropriate, shall -

- (a) make adjustment to the customer's account including interest or charges; and
- (b) notify the customer in writing of the adjustments made to his account.

**Financial institution to provide information**

28. Where a financial institution is of the view that the customer is liable for loss arising from any loss, misuse, theft or unauthorise use of a card or breach of access code security -

- (a) the financial institution is to make available to the customer, copies of any documents or other evidence relevant to the outcome of its investigation, including information from the log of transactions; and

- (b) the financial institution is also to refer to the systems log to establish whether there was any system or equipment malfunction at the time of the transactions,

and advise the customer in writing of the outcome of its inquiry.

Provided always that the financial institution will not be required to furnish any information that has a direct relation to or impacts the security of the financial institution or its system.

### **Information and advice on appeal**

29.(1) The complaint procedure of a financial institution shall contain information relating to -

- (a) the right of a customer to appeal against the outcome of his complaint to the senior management of a financial institution; and
- (b) the right of a customer to refer the complaint to the Banking Mediation Bureau, if he is not satisfied with the outcome of his complaint.

(2) The financial institution shall make known or make available the information in subparagraph (1) to a customer.

### **Breach of duties**

30. Where the financial institution, its officers or agents appointed fail to observe the -

- (a) allocation of liability under paragraphs 16 and 17; or
- (b) procedures on complaint, investigation and resolution under paragraphs 25 and 26,

and where such failure prejudiced the outcome of the complaint or resulted in delay in its resolution, the financial institution may be liable for the full amount of the transaction which is the subject of the complaint.

**Records of complaint**

31. A financial institution shall keep a record of complaints and their resolutions, so that aggregate data on the type, frequency and resolution of such complaints can be made available to Bank Negara Malaysia.

**Audit trails**

32. A financial institution shall ensure that their electronic fund transfer generates sufficient records to enable a transaction to be traced, checked and where any error has occurred, to be identified and corrected.

**PART VIII****MISCELLANEOUS****Privacy**

33.(1) A financial institution shall ensure that all information relating to an electronic fund transfer, affairs or an account of its customer shall not be disclosed unless permitted under the Banking and Financial Institutions Act 1989.

(2) No person other than, an officer of or agent appointed by, the financial institution that maintains the account, or the customer, may have access through an electronic terminal to information relating to electronic fund transfer, the affairs or an account of the customer.

(3) No electronic terminal shall be capable of providing any information relating to an electronic fund transfer, the affairs or an account of a customer unless -

- (a) the electronic fund transfer is operated by, an authorised officer of, or agent appointed by, the financial institution; or
- (b) the request for information is preceded by the entry of the correct customer's access code or card.



- 14 -

(4) A financial institution shall not provide any information relating to an electronic fund transfer, the affairs or an account of a customer unless the information is provided -

- (a) pursuant to a legal duty or responsibility; or
- (b) with the consent of a customer.

### **Banking Mediation Bureau**

34. A customer who is not satisfied with the outcome of a complaint made pursuant to these Guidelines may refer the complaint to the Banking Mediation Bureau.

### **Waiver of rights and greater protection**

35.(1) No agreement in writing between a customer and a financial institution may contain any provision that constitutes a waiver of any right conferred or cause of action created by these Guidelines.

(2) Nothing in these Guidelines shall prohibit any agreement, which grants a customer more extensive rights, or remedies or greater protection than those contained in these Guidelines.

### **ENQUIRIES**

Any enquiries on any aspects of the guidelines should be directed to:-

Jabatan Sistem Pembayaran  
Bank Negara Malaysia  
Peti Surat 10922  
50929 Kuala Lumpur

No Tel: 2988044

Legal Department  
10 December 1998